ebbits

Enabling the business-based
Internet of Things and Services

(FP7 257852)

D3.8 Legal, IPR and liability issues

Published by the ebbits Consortium

Dissemination Level: Public

SEVENTH FRAMEWORK
PROGRAMME

Project co-funded by the European Commission within the 7th Framework Programme
Objective ICT-2009.1.3: Internet of Things and Enterprise environments

Document version: 1.0

Submission date: 16 December 2013

Document control page

Document file:	D3.8 Legal, IPR and liability issues.doc
Document version:	1.0
Document owner:	Martin Knechtel (SAP)
Work package:	WP3 – Enterprise Frameworks for Life-cycle Management
Task:	T3.6 – Liability, IPR and regulatory issues
Deliverable type:	R
Document status:	☒ approved by the document owner for internal review ☒ approved for submission to the EC

Document history:

Version	Author(s)	Date	Summary of changes made
0.1	Jesper Thestrup (IN-JET), Villiam Vadja, Jozef Glova (TUK)	2013-10-30	First version with all background infor but without contribution from legal subcontractors, impact and conclusion
0.2	Eugenio Mantovani, Anna Moscibroda, Paul Quinn (researchers at VUB)	2013-12-13	Contribution from legal subcontractors Vrije Universiteit Brussels, Chapters 4, 5, 6, 7
0.3	Jesper Thestrup (IN-JET)	2013-12-16	Editing, added application cases
0.4	Jesper Thestrup (IN-JET)	2013-12-16	Prepared document for internal review
0.5	Sven Horn, Yves Martin, Martin Knechtel, Carsten Puschke (SAP)	2013-12-17	Added chapter with implications to running the ebbits platform in a productive environment Added conclusions
1.0		2013-12-20	Final version submitted to the European Commission

Internal review history:

Reviewed by	Date	Summary of comments
Pietro Cultrona (COMAU)	2013-12-19	Approved. Comau's lawyers find the document in line with what they expected
Matts Ahlsén (CNET)	2013-12-19	Approved

Legal Notice

The information in this document is subject to change without notice.

The Members of the ebbits Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the ebbits Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Possible inaccuracies of information are under the responsibility of the project. This report reflects solely the views of its authors. The European Commission is not liable for any use that may be made of the information contained therein.

Index:

1. Executive Summary

The ebbits platform will support business applications to automatically find information on the internet and real-world data from tags and sensors, and people. The ebbits platform can be used for on-line monitoring of a product in its entire lifecycle from the early production stage to end-of-life. These activities give rise to a variety of legal issues. This document gives a broad overview of these issues in order to illustrate the potential legal obstacles that a producer of an ebbits-like system may encounter. These can be conceptually described in terms of three areas as described below.

It should be noted, that this deliverable is neither intended as a complete legal discussion of the various legal frameworks covering all aspects of ebbits functionality nor is it intended to be read as a condensed and structured summary of the legal framework encompassing the operation of ebbits services. It is, however, intended as a directory of relevant juridical and legal topics that should be considered with deploying ebbits platforms and services in various setting.

The reader is invited to find the topic of interest and then study the EU and supranational regulations relevant for ebbits with some notes on differences in national implementations in the three major legal systems prevailing in Europe: The Common Law system represented by the United Kingdom, the German/Roman legal system represented by Germany and the Roman Law (Corpus Juris Civilis AD 529) system represented by Italy. These national representations should provide the reader with some insight into what should be considered in the specific Member State targeted for implementation of ebbits services.

1.1 Liability Issues

Liability issues can be various and complex. One important area involves the potential liabilities arising from faulty or defective products and/or services.

Product liability arises through the idea that a consumer has a right to legal redress for damage that is caused by a defective product.[1] A ebbits system may be considered as both a product and/or a service depending upon the context where it is provided.

An attempt was made at the European level to harmonise national laws on product liability. The primary source is Directive 85/374/EEC, the Product Liability Directive (PLD). This system represents largely the sole area where the liability of producers of products in Europe is harmonized. This contrasts with the situation concerning the provision of services where no major harmonisation has occurred. National laws will therefore apply when such issues are in dispute.

Defect is at the core of the PLD.[2] This contrasts with the notion of fault, which is at the core of many tort systems.[3] The notion of 'defect' is closer to a strict form of liability, as the claimant does not need to show that the manufacturer acted in an improper manner.[4] The PLD uses a standard of almost strict liability, meaning that product producers (and in some instances suppliers) can be held liable for defective products even where they themselves have not acted in an improper manner (e.g., where they could not be reasonably expected to know about the fault in question).

There are, however, certain defences available under the directive. One relates to the concept of 'discoverability'. This notion allows producers to escape liability when they can prove that it was not possible to discover the defect in question given the contemporaneous knowledge available.

[1] The concept of what product liability is can vary. In the UK it is taken to mean "that class of liabilities to which commercial manufacturers and commercial suppliers of goods are subject because a good has caused some form of actionable loss to either a business, a consumer or a bystander." See: Stapelton, 'Product Liability in the United Kingdom: The Myths of Reform', (1999), *Texas International Law Journal*, 34, 45-70 See also: Clarke, Product Liability (Sweet and Maxwell. 1989). In the European Court of Justice case of Commission v France C-52/00 [2002] ECR I-3827 the court stated that where the PLD applies, old pre-existing systems can not longer apply. This means that in Systems such a s France and Germany, the previous systems that were more beneficial to consumers no longer apply.

[2] Fairgreave & Howells, 2007.

[3] This includes for example the UK's system of general negligence.

[4] European Commission 'Third report on the application of Council Directive on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products' COM(2006) 496 Final

Suppliers can also escape liability for products they have provided if they are able to indicate the party that manufactured the product in question.

The PLD is important in the context of potential ebbits applications. This is because under a number of circumstances the ebbits system may constitute a 'product'. This may occur, for example, where the ebbits system has been provided to an automotive manufacturer. Where defects occur resulting in damage, e.g., to machinery or individuals, the producer of the ebbits system may be held liable. Similarly, in the agricultural production context, where defects lead to injuries to individuals (perhaps through the consumption of unfit food) or to private property, the producer of an ebbits system could face liability. It is important to note that the PLD does not regulate damage to commercial property or purely financial losses. The former could occur in the automotive manufacturing context, for example, where plant machinery is damaged or in the agricultural production context where loss of livestock occurs. The latter could occur where a defect in the ebbits system leads to financial losses, e.g., resulting from reputational harms or increased energy uses.

Where the PLD is not engaged, e.g., damage to commercial property, purely economic losses, or claims concerning the provision of services, recourse will have to be made to national systems of law (i.e., not harmonised by the EU) in order for claims to be settled.

There is considerable variation in national laws concerning liabilities in these areas. Each provides its own system of contractual and non-contractual liability. This document briefly looks at the systems existing in the United Kingdom, Germany, and Italy.

1.2 Intellectual Property

ebbits is likely to produce or use may intangible assets, such as computer programmes, literary or artistic works (e.g., images or literary descriptions), databases, valuable raw data, algorithms, industrial recipes etc.,. The Intellectual Property legal framework is thus crucial for ebbits in order to, on the one hand, secure its own investment and on the other, to avoid the infringement of Intellectual Property of others.

As regards protection of valuable intangible assets generated by an ebbits system, one needs to consider traditional IP protection, such as patents and copyright. Additionally, the legal framework for the protection of business confidential information and trade secrets is important.

Intellectual Property rights are regulated at the international and national levels. The European Union (EU) has adopted a number of legislative acts relating to the IP. European law complies with the obligations imposed by international law, but at the same time harmonises IPR further and often provides for a higher standard of protection then international conventions, in particular in the field of copyright.

In the area of copyright protection, harmonisation at EU level is provided mostly by Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (Information Society Directive), Directive 06/96/EC on the legal protection of databases (Database Directive), and Directive 2009/24/EC on the Legal Protection of Computer Programs (Computer Programmes Directive).

Copyright grants an exclusive right to control reproduction and communication to the public of literary and artistic works, as far as they are original and fixed in some material form. In the context of ebbits, the copyright may provide protection in respect of ebbits software, structure of database(s), other literary works (such as ebbits website or promotional material). No formalities are required for copyright protection. Copyright lasts for the limited period of time (in the EU, 70 years after the death of the author or from the date of first publication).

In the area of patent protection, currently there is no binding EU law on patents. Therefore the legal framework is comprised of regulation arising from both national and international laws (the most relevant act being the Council of Europe European Patent Convention of 1973). The patent will protect any invention that has a technical character, providing that it is new, that it involves an inventive step and is susceptible of industrial application. The patent protection lasts for a limited period of time (20 years under the European Patent Convention). It requires formal filling with competent authorities. Filing implies disclosure of information regarding the invention in question, and may involve significant costs. Certain subject matters are excluded form patent protection. In Europe (under European Patent Convention) the most significant exclusions form patentability in the context of ebbits relates to scientific theories, mathematical methods, business methods, and ordinary computer programmes. The patentability of computer-related inventions is controversial. The patent application requires formal filling.

As far as data and knowledge ownership are concerned, patents and copyright do not provide for ownership of data or knowledge. Hence, neither patents not copyright will protect algorithms, mathematical methods, know-how, industrial recipes, or valuable raw data. Such assets may constitute confidential information and trade secrets. Given the very limited harmonisation of laws on business confidential information and trade secrets on the international level, and awaiting adoption of EU laws in the field, the protection of the business confidential information and trade secrets is provided by the national law of each Member State.

The legal protection of trade secrets differs from intellectual property protection. In particular, the former does not create an exclusive right. This means that, for instance, the trade secret cannot be enforced against a third party who has obtained the information constituting the trade secret in good faith.

As per IP liability, the ebbits platform may use third parties' data, information and knowledge, as well as copyrighted works or inventions protected by IP. In order to avoid the potential liability for infringement, ebbits should secure the licence from the copyright or patent holder.

ebbits may also be under an obligation to protect the trade secrets or confidential information of third parties. ebbits can and should aim to preserve the confidentiality and secrecy of the information it handles by preventing its accidental disclosure. ebbits should also be able to control who gains access to information. ebbits should be careful in information sharing, e.g., by providing information only on a need-to-know basis, by subjecting it to scrutiny in terms of confidentiality requirements and by applying technological measures protecting such information.

Digital Rights Management is used in relation to technological systems that define, manage and protect the rights of access to and use of digital content (e.g. the music or audio file, text and e-books, etc.). DRM defines how and by whom such content may be used, thus implementing the copyright licenses or ensuring the security and confidentiality of data. In the context of ebbits, DRM that is used to protect copyrighted material, such as software, enjoy legal protection under Copyright law. DRM might also be used to manage confidential information and to ensure data security. In these contexts, DRM systems may ensure protection of trade secrets, but also enable that data processing complies with privacy and on data protection laws. Finally, the use of DRM may pose some privacy concerns when its leads to collecting or processing of personal data. In such cases it is advisable ebbits is equipped with a DRM protection system with privacy enhancing technologies (PETs).

1.3 Data Protection

Protection of privacy and personal data in the European Union has been extensively harmonised. Privacy and data protection are recognised as fundamental rights under the EU Charter of the Fundamental Rights (CFR), they are recognised in the Treaty on the European Union (TEU) and in the Treaty on the Functioning of the EU (TFEU), and in secondary legislation, of which Directive 95/46/EC is the most stringent instrument, currently undergoing a comprehensive revision.

Data protection is a set of safeguards promoting the transparency and accountability of government and private-sector record holders. While privacy laws proscribe any processing of privacy personal data "unless" necessary, the rationale of data protection is the opposite: normal personal data (as opposed to precise categories of sensitive personal data, mentioned below) is free to be moved and processed, provided that transparency conditions are respected

EU data protection law provides a number of important principles, rules, safeguards, recommendations, good practice, etc. that are applicable to ebbits applications. This document highlights four areas of interest to ebbits: workplace privacy, profiling, data breach notification, and privacy and data protection impact assessment (DPIA).

In the area of workplace privacy, data protection law protects the personal data associated (e.g., through RFID tags) with products in their life cycle. In the context of the ebbits project this means that where tags store information about individual workers, such data should be processed fairly and lawfully and not exceeds the purpose they were originally collected for. Individual explicit consent of the worker should be obtained, in particular if sensitive data are collected about, e.g., the individual worker affiliation with trade union or health status. Management should also engage workers associations, e.g., trade unions. It is important to involve workers and their associations to discuss the potential privacy implications of, say, RFID tags. (See below on Privacy Impact Assessments).

Second, the issue of profiling consumers: Profiling means collecting and using pieces of information about individuals to make assumptions about them and their future behaviour. This is possible through so called profiling algorithms. In the context of ebbits services, consumers must retain the right to object profiling. The right to object should be accompanied by the right to be informed about the techniques and procedures used for profiling, particularly in advertising. Consumers should be informed of the possible consequences of profiling techniques applied to them. Since profiling algorithms are often protected as "trade secrets", this may lead to the risk that unreliable profiling is used without the required checks and balances to counter its defects.

Third, in the context of an approach focused heavily on the 'Internet of Things', the chances of data being lost or leaked is higher. For this reason, it is recommended that ebbits services incorporate in their system architectures data breach notification procedures. It is equally important to keep contact records for customers up to date, ensuring that information is current and accurate. This will avoid missed notifications or notifications being issued to the wrong data subject. Additionally, operators may want to consider the preparation of a list of examples of potential unexpected incidences and seek guidance in advance from authorities in order to avoid any future confusion.

Fourth, Privacy Impact Assessments (PIA): Privacy Impact Assessment is a process for assessing the impacts on privacy of a project which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts. In the context of ebbits products and services, it is advisable to carry out an initial analysis seeking to determine whether and to what extent personal data are going to be processed. This should be done in coordination with stakeholders, e.g., trade unions and consumer organisations. Should privacy risks or concerns arise, a risk management procedure should identify the appropriate mitigation measures depending on the likelihood and magnitude of the risks and concerns in question.

1.4 Conclusion and Impact on the ebbits Platform

The important question to the ebbits project partners are what implications we draw from this deliverable. We discuss that in Chapter 8. We found that technology-wise, the ebbits platform does not need significant extensions or changes. However, there are several organizational implications that need to be taken into account when running the ebbits platform productively.

To mention some examples: it should be possible to deactivate RFID tags or remove personal information of workers and workers should be involved to discuss the potential privacy implications from the beginning on; search queries by users and user profiles with preferences contain private information and will be protected by the ebbits platform; etc. The detailed list of all implications we found is provided in the corresponding chapter.

The results of this deliverable will help the consortium to advance the ebbits platform in the last project year so that it can be used as the basis of a productive system.

2. Introduction

The ebbits platform will support business applications to automatically find information on the internet and real-world data from tags and sensors, and people. The ebbits platform can be used for on-line monitoring of a product (or any other artefact in the IoT) in its entire lifecycle from the early production stage to end-of-life.

The ebbits architecture is deployable in many different domains characterised by different forms of production and thus different challenges of optimisation and coordination in the physical world: Process industries (e.g. pharmaceutical), stream industries (e.g. meat production) and assembly industries (e.g. automotive manufacturing).

In automotive manufacturing, an ebbits application may allow a large number of stakeholders (e.g. car manufacturers, sub suppliers, system integrators, maintenance organisations, etc.) to perform real-time monitoring of machine states across production lines and with real-time decision support and subsequent changes in manufacturing execution.

In the food industry, the ebbits applications can be used to trace food along the food chain from "farm to fork". Data are automatically collected from various actors (farmers, slaughter houses, supermarkets, etc.) An ebbits application will allow authorities, food chain actors, retailers, and consumers to obtain comprehensive and reliable product information of the life-cycle history of the food.

2.1 Background and Overview of the ebbits Project

The ebbits project aims to develop architecture, technologies and processes, which allow businesses to semantically integrate the Internet of Things into mainstream enterprise systems and support interoperable real-world, online end-to-end business applications. The ebbits platform thus enables the convergence of the Internet of People (IoP), the Internet of Things (IoT) and the Internet of Services (IoS) into the "Internet of People, Things and Services (IoPTS)" for business purposes.

The ebbits platform will support interoperable business applications, such as life cycle management and energy optimisation, with context-aware processing of data separated in time and space, information and real-world events (addressing tags, sensor and actuators as services), people and workflows (operator and maintenance crews), optimisation using high-level business rules (energy and cost performance criteria), end-to-end business processes (traceability), or comprehensive consumer demands (product authentication, trustworthy information, and knowledge sharing).

As part of the project, non-functional socio-economic requirements related to ethical and legal realms have been investigated in order to secure the deployability of the ebbits platform in real life settings.

Important requirements derived from liability analysis and IPR issues must be included in order to convince potential operators and users of the ebbits services of its safe deployment. Further aspects of inclusion and data protection requirements i.e. ensuring that individuals should have the possibility to control access to his or her personal information and to construct his or her own public persona are also of great importance.

2.2 Purpose, Context and Scope of this Deliverable

The purpose of this deliverable is to describe which legal perspectives can be applied to the operation of the ebbits service platform. The deliverable first provides a basic overview of the ebbits ecosystem identifying relevant actors and their interrelations in two domains, manufacturing and the food chain. Since the legal work is outside the competence of the ebbits partners, a legal expert has been brought in to provide the legal descriptions.

It should be noted, that this deliverable is neither intended as a complete legal discussion of the various legal frameworks covering all aspects of ebbits functionality NOR is it intended to be read as a condensed and structured summary of the legal framework encompassing the operation of ebbits services. It is, however, intended as a directory of relevant juridical and legal topics that should be considered with deploying ebbits platforms and services in various settings. The reader is invited to find the topic of interest and then study the EU and supranational regulations relevant for ebbits with some notes on differences in national implementations in the three major legal systems prevailing in Europe: The Common Law system represented by the United Kingdom, the German/Roman legal system represented by Germany and the Roman Law (Corpus Juris Civilis AD 529) system represented by Italy. These national representations should provide the reader with some insight into what should be considered in the specific Member State targeted for implementation of ebbits services.

Chapter 3 provides examples of typical life-cycle and energy optimising applications with the aim to give the reader insight into the legal issues that needs to be considered by operators, service providers and all the involved actors in a real world implementation. These legal topics are then discussed at the EU level as well as at the national level in the remaining parts of the deliverable.

Hence Chapter 4 describes the methodology used for addressing the legal issues and the scope of the work undertaken by the legal experts.

Chapters 5, 6 and 7 provide the discussion of the legal framework for managing IPR and liability issues in Europe related to ebbits as presented by the legal experts. Chapter 5 discusses product liability with a focus on liability foreseeable at the time of manufacture and on liabilities arising as a consequence of malfunctioning parts of the ebbits platform. Chapter 6 discusses the realm of Intellectual Property Rights protection in a distributed, digital environment. It outlines the various instruments for protection and with a particular view to ebbits ebbits applications where principles of DRM (Digital Rights Management) can be put in play. Finally, chapter 7 looks at issues of ownership and protection of data, including the protection of human data.

The ebbits partners have evaluated the impact of the legislative and regulatory constraints on the ebbits architecture and its major components. The results of these evaluations are provided in chapter 8.

Finally, conclusions on the legal, IPR and liability issues are discussed in chapter 9.

2.3 Subcontracting Legal Expertise

The Document Owner SAP (and theother industrial partners in the consortium) have in-house expertise, but cannot undertake the work because the in-house lawyers are not allowed to work on public matters. Partner IN-JET does not possess legal expertise to carry out the expert work on describing the legal framework. Consequently it was decided to seek external expertise to perform this part of the work, which was discussed and approved at the ebbits review meetings on 8 May 2013 and again on 14 November 2013.

The consortium has subsequently carried out a bidding procedure involving three independent and reputable experts in two different member states. After careful examination, the ebbits Project Board decided to award the work to Vrije Universiteit Brussels - Law Science Technology & Society (LSTS), Department of Metajuridica - Faculty of Law. The offer was fully compliant with the need of the project and included both EU law perspectives and implementation details in three different Member States: United Kingdom, Germany and Italy. These member states represent fundamentally different legal systems in Europe and, moreover, the industrial ebbits partners have strong interest in Germany (SAP, Fraunhofer) and Italy (COMAU).

Due to the extended time for preparing and conduction the bidding process (over the summer 2013) the deliverable has been delayed four months compared to the original plan. This delay has no effect on the other work to be performed in the ebbits project.

3. The ebbits eco-system

This section is provided as context for readers that are not familiar with the ebbits platform. It provides the background and identifies the potential legal issues providers and actors may expereince when deploying an IoPTS platform like ebbits. If you are familiar with ebbits, you may skip this chapter and go directly to chapter 4 or 5 for the legal discussions.

3.1 The Business Environment

The IoT will grow to 26 billion units by 2020[5]. Those billions of devices will be able to communicate with each other, with users or other people, and with enterprise and public information systems and thus open the way towards the Internet of Things, People and Services. The multitude of tags, sensors, and actuators provide physical world information to be used to optimise business processes and create new business opportunities. However, given the enormous amount of heterogeneous devices, sensors and actuators embedded in systems already existing in the market, the diversity of the producers and manufactures, the different clock speed of technology (from several decades to some months), and the potentially global distribution of final products (once they leave the controlled manufacturing and distribution environment), there is a pressing and clear need for technologies and tools that can add, implement and exploit the intelligence and interoperability embedded in individual devices, manufacturing environments and global ubiquitous networks.

Suppliers and users of enterprise systems must be able to collect information from the physical world, reason and reflect on this information, combine it with existing explicit or tacit knowledge and act on the real-world through actuators. They must be able to integrate the Internet of Things into their optimising systems, i.e. management of workflows, people, processes, assets, data, information and knowledge, and turn them into useful, value-added business services.

Producers of various components, devices and systems are increasingly facing the need for networking their products with enterprise systems in order to provide higher value-added solutions for their customers or because customer centred demands and demographic changes, including shortage of labour, require much more focus on intelligent solutions, where the complexity of the system is hidden behind user-friendly interfaces.

Producers of consumer products, such as foodstuff or pharmaceuticals, are already today facing increasing demands and strict regulatory requirements for authentication, originality and traceability of their products. This requires vast access networks in order to reach consumers where they need the information and integration with data sources that may be widely temporally dispersed (between time of manufacturing and time of consumption). Authentication and traceability applications would be required to seamlessly interoperate with backend systems using existing and widespread wireless terrestrial networks and smart home environments.

In conclusion, the enterprise world at large needs a platform to enable, deploy and maintain the *Internet of Things and Services* and integrate the physical world in their business management platforms and enterprise systems. It also needs a *smart* platform for reduced time to market, faster deployment of service changes, customisation and scalability, while at the same time building on their enormous installed base of industrial assets. It needs to have context-aware *services* processing physical-world events and performing action on the physical world. And it needs it for production and energy optimisation, authentication and traceability, and a wealth of other high-value intelligent services aimed to improve their business performance in the future. It is the aim of the ebbits platform to fulfil these needs.

[5] http://www.zdnet.com/internet-of-things-devices-will-dwarf-number-of-pcs-tablets-and-smartphones-7000024229/

3.2 The Platform

The ebbits platform bridges the gap between virtual enterprises and public information systems, human users and "things" in the physical world. The ebbits platform creates a ubiquitous communication infrastructure that automatically and dynamically connects to sensors and devices in the physical world in e.g. manufacturing facilities or in private smart homes. It further connects to mainstream backend information systems, public authentication systems and regulatory information sources using semantic web services. It finally connects to human users in dispersed geographical locations such as professional users in technical support, field service and other business environments as well as ordinary consumers in shops or at home.

Physically, the ebbits platform consists of subsets of production servers for data management, event management, security, application execution and communication. All servers interoperate in an open architecture on the basis of web services and are thus completely platform agnostic and scalable. A software development toolkit allows for rapid development of new ebbits applications. The platform is visualised in Figure 1.

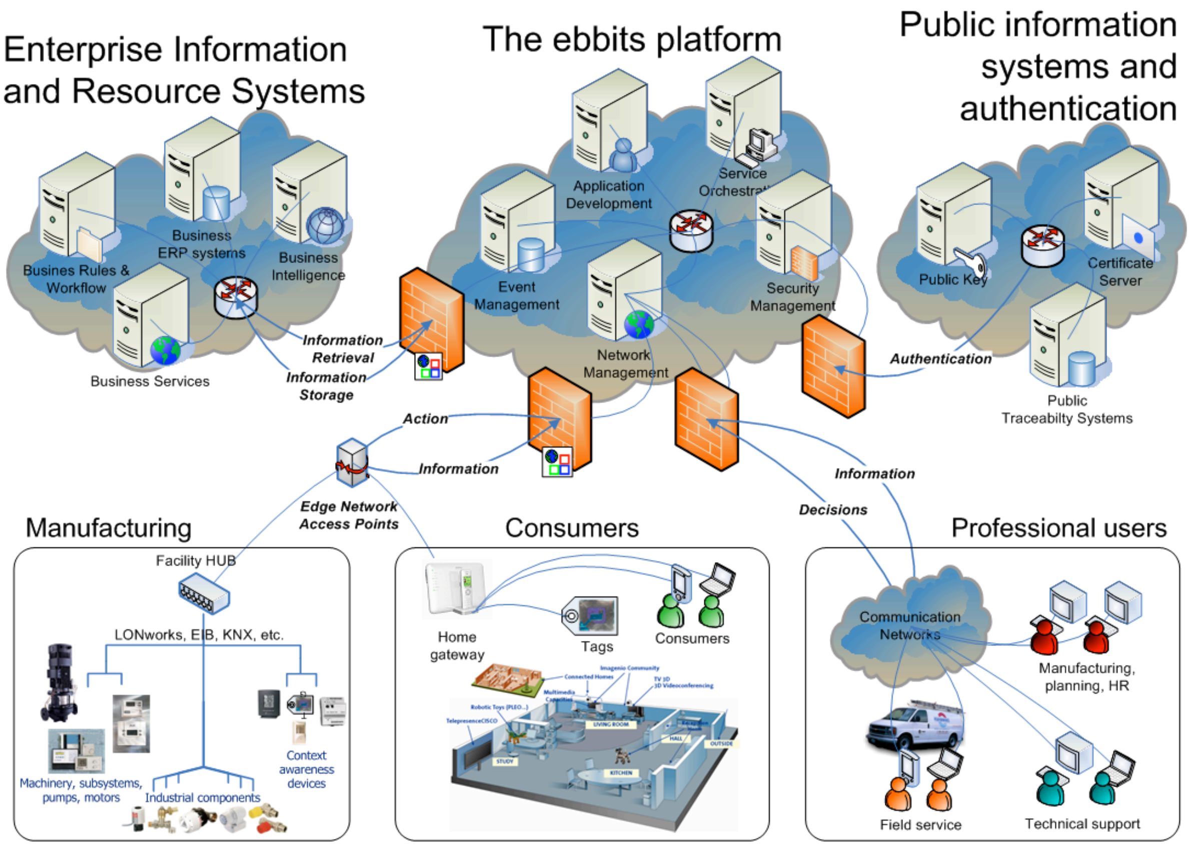


Figure 1 The ebbits platform concept

Devices (tags, sensors, terminals, systems, sub-systems, etc.) are seamlessly connected to the ebbits platform as Web Services that proxy the functionality of the device. This is obtained either with a middleware embedded in the device itself or by virtualisation of the device e.g. on a network node. The middleware employs semantic technologies that automatically discover and configure the physical devices irrespective of their underlying communication protocol and thus enables every device to participate in intelligent service orchestration deployed by the enterprise management system.

The device interconnects with other devices in the environment that can record contextual information about the parameters in the physical world. Data are pre-processed and formatted in the active edge network access layer nodes/gateways. The gateway can handle virtualisation, authentication, real-time monitoring and event handling and other services, which are needed during periods of outage (non-connectivity).

The gateway also manages personalised feedback to business professionals, adapted to the available user terminals, as well as self-monitoring and autonomous regulation of devices and systems in the physical world, e.g. preventive service and maintenance monitoring. For devices and sub-systems not capable to operate web services (due to resource constraints or proprietary concerns), the gateway also dubs as a platform for virtualisation of devices.

The ebbits platform also connects into smart-home environments for consumers and private users. Identification and authentication of products with RFID tags is done automatically and consumers can be warned about unsafe or counterfeit products, "best-before" dates, end-of-life precautions, etc. Consumers can also inquire product life-cycle information (traceability).

Throughout the ebbits platform, data are transmitted securely to and from nodes through fixed or mobile public and/or proprietary networks.

3.3 Lifecycle Management

The ebbits platform supports end-to-end business applications based on connectivity to and monitoring of a product in its entire lifecycle, i.e. from the early manufacturing stage to its end-of-life. Real-time life-cycle management implies that the manufacturer has on-line access to the product from the moment it starts the production process and until its effective end-of-life. If this would be possible for all products, it would dramatically change the business performance of a wide range of industries. Equipment and machinery already today features on-line asset management: From manufacturing equipment, large building heating and cooling installations to vending machines and pumps; all leading manufacturers have on-line access capabilities to their products. With the IoPTS, this capability will be extended to also include smaller products, including consumer products such as food and pharmaceuticals.

The functionalities and sustainability of the ebbits platform will be demonstrated in two domains.

One domain involves production optimisation and energy awareness in manufacturing industries. The aim of this demonstration is develop and validate an ebbits online optimisation business application using an enhanced optimisation metrics by adding energy consumption and CO_2 emission to the traditional efficiency metrics used in TPM (Total Productive Maintenance) and LEAN Manufacturing. The ebbits platform will demonstrate interoperability of traditional large scale manufacturing equipment with a range of heterogeneous and proprietary auxiliary equipment such as energy monitors, environmental sensor networks, etc.

The other field trial involves life-cycle management in the food chain. The ebbits platform will support continuous monitoring of food products regardless of its actual geographical location. The application will show how comprehensive traceability of products can be devised based on widespread availability of wireless networks and smart home infrastructures. Information will seamlessly be collected from farms, food processing plants, the logistic chain, and public databases and presented to the consumer in a usable and inclusive way.

3.4 Typical Applications in the Manufacturing Domain

The ebbits applications will have to manage disperse and heterogeneous data stores by using e.g. semantic data mining techniques; it will have to manage off-line data in data repositories and real-time data from e.g. sensor networks; it will have to manage various types of public and proprietary networks with different access control paradigms; it will have to manage feedback to a multitude of human interaction terminals such as desktop and mobile platforms; and it will have to manage security aspects, billing aspects, IPR issues and many other non-functional requirements.

3.4.1 VMA Energy and Climate Impact Data

This application is aimed at collecting and aggregating energy data across the Vehicle Manufacturing and Assembly (VMA) processes for use in life-cycle assessment (LCA) of the vehicle's life-cycle. The overall purpose of such LCA is to develop an environmental "picture", where life-cycle burdens, such as energy, CO2 emissions, and raw materials, are quantified and evaluated over all stages of the vehicle's life-cycle. Hence, tradeoffs between life-cycle stages can be accounted for, resulting in more holistic assessments of product systems and often illuminating improvement opportunities. For example, vehicles made lighter by substituting materials like aluminium and composites for steel do indeed have higher fuel economy (use phase), but at the same time a part of that benefit is offset by the generally higher production energies of alternative materials (material production stage).

For vehicles, the burdens for the material production and vehicle operation stages are the largest and best understood. Though less well understood, the burdens for the part manufacturing and vehicle assembly (VMA) stage are the next largest in magnitude, and hence the focus of this application. Because no real-time data has been available for individual car models and individual cars, LCA specialists have been developing complex models that can predict energy and CO2 data estimates from generic models of different types of vehicles. Such model is the Greenhouse gases, Regulated Emissions, and Energy use in Transportation (GREET) model developed by Argonne National Laboratories in the US (Sullivan 2010).

The ebbits application will be deployed to collect the energy and CO_2 data from a potentially large number of sub processes and sub suppliers and organise the data in a VMA Energy and Climate Impact sheet as shown in Figure 2. The aim of the ebbits application is to 1) improve the accuracy of the VMA model, 2) make it specific to a particular car model or even the individual car, and 3) make it available online to various stakeholders.

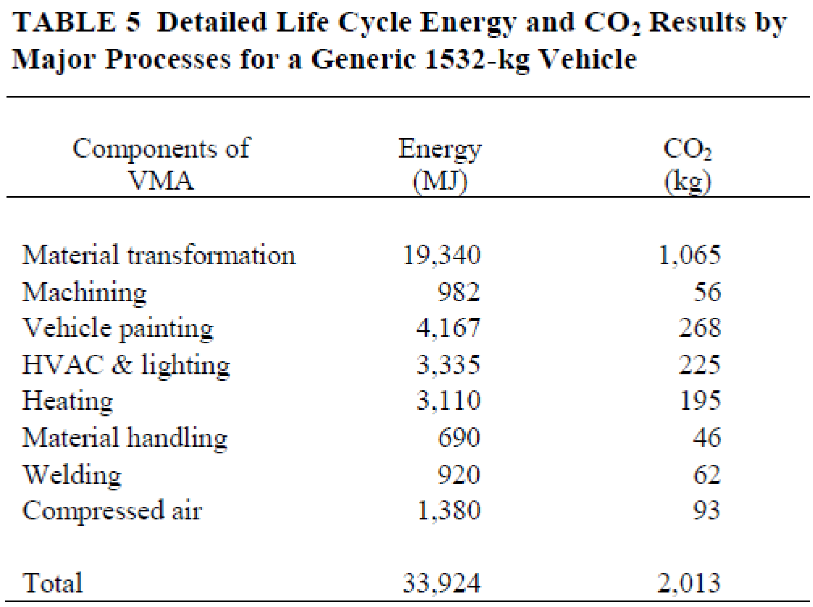


TABLE 5 Detailed Life Cycle Energy and CO_2 Results by Major Processes for a Generic 1532-kg Vehicle

Components of VMA	Energy (MJ)	CO_2 (kg)
Material transformation	19,340	1,065
Machining	982	56
Vehicle painting	4,167	268
HVAC & lighting	3,335	225
Heating	3,110	195
Material handling	690	46
Welding	920	62
Compressed air	1,380	93
Total	33,924	2,013

Figure 2 Energy consumption in VMA (Source: Sullivan 2010)

Some legal issues related to this scenario are:

- How is proprietary data carried down the supply chain while maintaining confidentiality?
- How is liability defined for damages caused by missing, incorrect, or incomplete data from other parts of the supply chain?

3.4.2 Predictive Maintenance Monitoring

Taking care of an automatic plant used to be an extremely difficult task. Employees in the plant needed years to learn how to become aware of anomalies that might cause production shut-downs. In some cases employees developed the ability to "listen" to the sound of the machine to perceive changes in the repetitive cycle and almost prophetically forecast potentially disastrous situations.

An all-encompassing monitoring system now detects any kind of internal and external variation in the production environment. Externally it detects financial fluctuations, providing information on the long-term strategy to be adopted; it detects the logistic situation, adapting the tactical production plan. Inside the plant, it detects the production flow status, faults on the machines and manages anomalous situations alerting the maintenance crew to intervene. The data are retrieved immediately from both external and internal environment and data flow is real-time so that decisions can be made immediately when any change in the operating conditions is noticed.

Some legal issues related to this scenario are:

- How are private data of the operator's moves and actions on the shop floor protected?
- Who is liable if the preventive action is not performed in time due to a malfunctioning of the system? Is it the network supplier? Or the application developer?

3.4.3 OEEE Production and energy optimisation

The application has been described in the predecessor of this Deliverable (D3.6 Business modelling concepts M24). For convenience we inserted the description from there, readers already familiear with this application may skip this chapter.

Energy management approaches and measurement and verification protocols are becoming more and more a significant issue in manufacturing environment. Nowadays energy data and information are not easily available and often they are disaggregated, thus their analysis and the consequent optimization strategies are very difficult to be implemented. In general when the energy managers try to implement energy monitoring applications, they find themselves drowning in the volume of data generated. Thus it becomes important to define and apply Key Performance Indicators (KPIs) to summarize volumes of data into a few critical "nuggets" of actionable information.

Figure 3 Shop floor operator

The business framework for production and energy optimisation is described in details in the deliverable D3.4 Business framework for online OEEE applications for production and energy optimisation. Only the highlights of this business domain will be provided here and readers are referred to the deliverable for more information.

The ebbits architecture is deployable in many different manufacturing domains characterised by different forms of manufacturing and thus different challenges of optimisation and coordination in the physical world: Process industries (e.g. pharmaceutical), stream industries (e.g. meat production) and assembly industries (e.g. automotive manufacturing). However, all these considered scenarios are characterized by dynamic changing conditions due to mass product customization, the constant shortening of product life-cycle as well as plant maintenance and/or modernization.

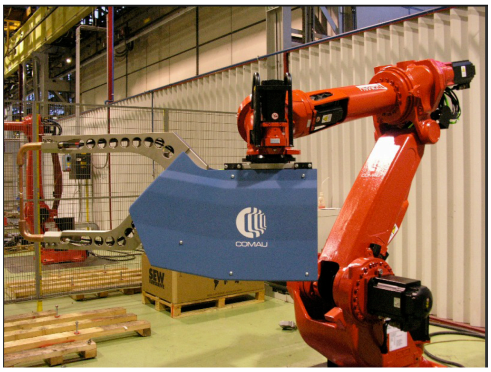


Figure 4 Comau Robot NJ4 with Versa Gun

For simplicity, the assembly industry has been selected as the industrial domain to be used for the deployment prototypes in the ebbits project.

Worldwide, industry consumes almost one-half of all the commercial energy used (IEA, 2012) and is responsible for roughly similar shares of greenhouse gases. An increasing number of manufacturing companies are facing a supply chain, which is demanding quantification of the carbon footprint and demands for future reductions. In order to stay competitive in the 21st Century; companies need to be include sustainability in their production optimisation schemes.

Hence, a business application that could help plant managers and production line managers to optimise the energy consumption of the process is very much needed. The ebbits project will develop a totally new optimisation metrics by adding energy to the commonly used OEE index, thus creating a new key index, the OEEE (Overall Equipment and Energy Efficiency).

By combining the OEE KPI calculation with the energy management technologies it is possible to define a new KPI: the OEEE Overall Equipment and Energy Efficiency index.

The OEE index is used in most manufacturing companies as a key metric in TPM (Total Productive Maintenance) and LEAN Manufacturing to provide a consistent way of measuring the effectiveness of the production. The OEE index is the product of three factors: Availability, Performance, and Quality.

The OEE index is a pure economic efficiency metric. However, manufacturing is a major consumer of energy. It is becoming increasingly clear that the quantitative assessment of various factors affecting industrial energy consumption is essential for forecasting industrial energy demand and particularly estimating energy requirements of alternative manufacturing strategies (Liu 2005).

In order to compute the OEE and OEEE indexes, the required information should be gathered from the field. For such reason, we propose a first data collection strategy that could be deployed at "production station" level and then replicated to stations which compose a production line and then extended to the whole plant.

The new OEEE (Overall Equipment and Energy Efficiency) index will have the following four components:

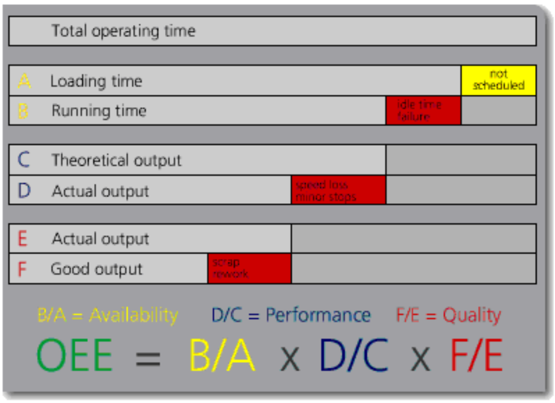


Figure 5 Calculation of OEE index

Availability looks at the down time loss, which is the time the production is stopped, compared to the planned production time. Availability is a function of equipment failures, material shortages, and changeover time.

The *Performance* component is also a function of down time, changeover time and speed loss, i.e. factors that results in the process operating at less than maximum speed due to machine wear, misfeeds, and operator inefficiency.

The *Quality* component depends on the amount of produced items that fails to meet quality standards and thus will have to be either rejected or reworked.

The *Energy* component is a function of the total energy consumption used in the production process.

Basically, almost all of the data needed to compute these indexes are located in two subsystems of the manufacturing scenario: PLCs and ERP systems. The latter contains the information related to "planned" activities (e.g., planned production time), while in the former, PLCs are in charge of gathering all the complementary "measured" data (e.g., energy consumption, uptime, etc.).

The computation of the OEE and OEEE indexes require different types of information to be collected, thus it is important to identify which data is needed for each one of the indexes, and according to their nature and requirements, devise the best strategy (where, when and how) to extract such information.

Some legal issues related to this scenario are:

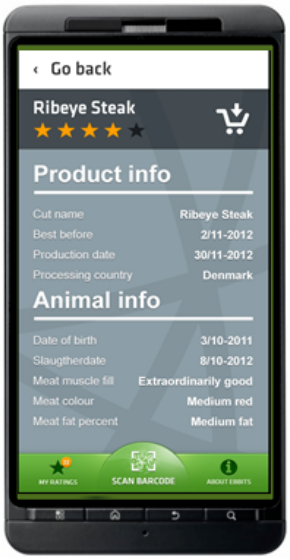
- Who is liable if the re-planning of production is not performed correctly due to a malfunctioning of the system?
- How are the proprietary data of suppliers in the supply chain protected and how are IPR handled for proprietary/patented processes?

3.5 Typical Applications in the Agriculture Domain

3.5.1 Food traceability

The secure tracking of food from the production place to the consumer is one of the important issues of an ebbits IoT application within the agriculture domain. From "farm to fork traceability" of each package of food is being required nowadays. The application can help a consumer to trust that the food is safe for consumption. The entire food chain and actors within these processes are influenced by new technologies such as high-frequency RFID tags, different sensors or actuators.

The ebbits platform provides the middleware which helps to implement traceability for food products based on a voluntary exchange of data from producers and processors to the consumer. The main objective of ebbits will be to collect and compile all the necessary product life cycle data and to make this data available to external applications via ebbits services, in order to provide product traceability. Data sources and services include external databases and human actors (for data inputs or manual service/decision making) as well as various IoT devices such as RFID tags, temperature sensors or actuators.



‹ Go back

Ribeye Steak

★★★★★

Product info

Cut name	Ribeye Steak
Best before	2/11-2012
Production date	30/11-2012
Processing country	Denmark

Animal info

Date of birth	3/10-2011
Slaugtherdate	8/10-2012
Meat muscle fill	Extraordinarily good
Meat colour	Medium red
Meat fat percent	Medium fat

Figure 6 Food information at the Point of Sale

The challenge in food traceability is that the benefit from using individual identification of animals is the total sum of effects all the way through the production and distribution chain from feed production, through growing the animals on the farm to slaughtering and distributing and finally ending up in the hands of the consumer.

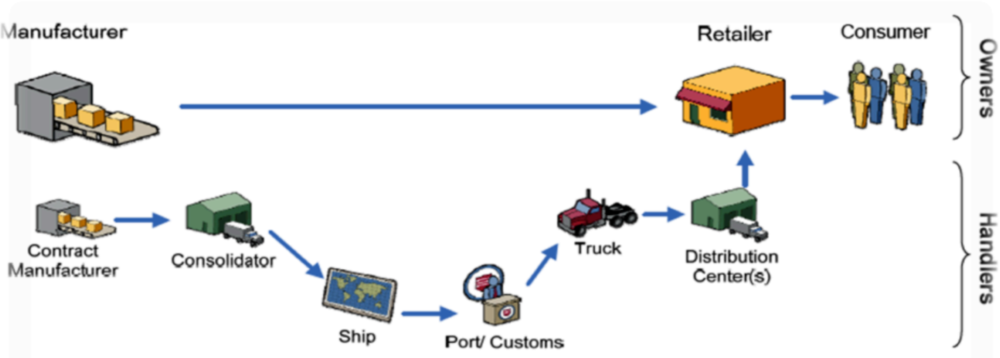


Figure 7 The complex chain of events when distributing products (Taillard 2011).

Each of the involved actors provides information. These can contain sensitive information and details of the production processes which might be considered as intellectual property or should cover information about supply chain. Almost all the activities in the food traceability eco-system has to reflect the current legal policies and each of the mentioned actors should be aware of their duties and responsibilities according to ownership and handling with provided data.

But as the report (Taillard 2011) describes there are many trends affecting the requirements to a traceability implementation. It identifies the following trends as the most important ones:

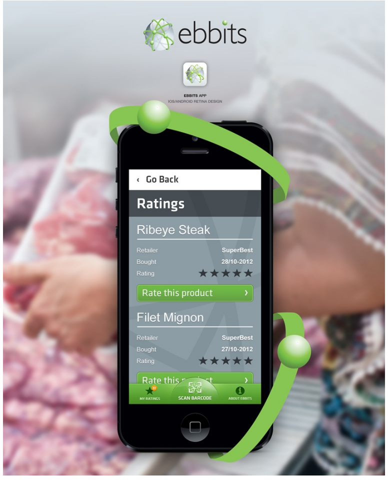
- Societal Trends – Increased demand for information and options to share experiences/ knowledge through social media.
- Technology Trends – Many have powerful smart phones with high speed internet access in their pocket that is underutilized.
- Economic Trends – Easier for producers to create brand identity and accessing loyal consumers.
- Environmental Trends – This does also help branding of products for socially responsible companies.

- Political Trends – Increased consumer safety and access to consumers.

Some legal issues related to this scenario are:

- Security risk when counterfeit products are mixed with genuine products. Counterfeited products can carry genuine (duplicated) identification codes. Who is liable for damage?
- Many production data (e.g. animal breeding) are proprietary and the supplier of these data will request that ownership be maintained and that data are only shared with actors who have the right to see them.
- Some information is from governmental databases which must be protected. Who is liable if data are leaked from other suppliers?

3.5.2 Consumer Experience Network



‹ Go Back

Ratings

Ribeye Steak

Retailer SuperBest
Bought 28/10-2012
Rating ★★★★★

Rate this product ›

Filet Mignon

Retailer SuperBest
Bought 27/10-2012
Rating ★★★★★

Rate this product ›

Customer satisfaction and loyalty are key elements that also determine the success in agriculture domain. The Internet of People or social media is a new driver in building customer satisfaction and improving loyalty. From this point of view, the feedback from the end-customers is very important in branded food. The traceability scenario demonstrates a consumer experience, which is the useful extension of the product lifecycle.

The service is provided through a *Consumer App* developed on the ebbits platform. The application is focused on creating a mobile consumer experience to retrieve all accessible information about a meat product at the point of sale. The mobile phone application uses QR codes, which are easy and cheap to generate and placed on meat products.

The application consists of a series of pages for user interaction. The information page shows the most important information about the product in a compact and user-friendly way. This is the first page the user sees after scanning the meat.

The producer screen informs about production conditions on the farm where the meat originates. The intention is that the farmers themselves should be able to add descriptive information.

After buying a piece of meat (the consumer has to select that from the information page) the consumer is prompted by a popup message (same evening that the consumer bought his meat) which asks the consumer to rate the meat, see. The user can also choose to rate the meat at a later point in time. It is not possible to rate the meat more than two days after "best before date".

Some legal issues related to this scenario are:

- Intellectual property rights of product information (recipes, breeding information) needs to be protected.
- Consumers' privacy needs to be protected (from unwanted advertising)
- Brands may be trade mark protected.
- Who is liable if the consumer is given a poor advice? Is it the shop that provides the service and sells the meet?

4. Methodology

The objective of the analysis is to identify and describe legal consequences related to the ebbits service platform. The analysis includes product liability issues for the involved actors in the value system, related to the protection of Intellectual Property Rights as well as legal issues concerning the monitoring and storing of data related to people involved in the IoTPS (Internet of Things, People and Services) ebbits eco-system.

4.1 Product Liability

Many different producers and service providers will provide different parts of the final ebbits service. When a defective device or an erroneous network transmission causes damages to the product or stops the manufacturing process, it could be very difficult to determine which producer or provider to hold liable for the damages caused and whether this producer has indeed committed a fault that caused the damage. Another threat is the leaking of proprietary and private data caused by insecure software or network components.

Council Directive 85/374 concerning liability for defective products stipulates that producers are jointly and severally liable for defective products. However, the directive does not apply to services and it is unclear whether the Directive could be invoked in the case of ICT products. In addition, the directive does not give guidelines if a product is defective when it insufficiently protects against privacy violations or when it easily allows identity theft. Other questions concern whether the provider of the software can be held liable and to what extent this liability can be waived in general contractual terms and conditions. Questions of liability shall be addressed focussing on both *direct liability* and *indirect liability.*

4.2 Intellectual Property Rights (IPR)

Intellectual property rights such as copyrights, patents, etc., provide the legal protection upon which stakeholders rely to protect knowledge, which becomes openly accessible through the ebbits platform. Digital technologies allow unlimited copying and dissemination of knowledge so without adequate protection and enforcement authors may not make their knowledge available. The legal framework for digital content IPRs in the EU is established by the Directive on the Harmonisation of Copyright and Related Rights in the Information Society (2001/29/EC). The Directive also addresses the use of Digital Rights Management[6] systems (DRMs) that can be used to enforce usage rules set by right holders or prescribed by law for digital content. They can also facilitate legal copying and reuse of content by establishing a secure environment in which right-holders are remunerated for private copying, on-line content is paid for, and illegal copying is prevented. This subtask will present the EU framework for IPR law that is applicable in the contexts of ebbits and illustrating IPR related problems.

4.3 Ownership and Protection of Data

Ownership of proprietary data in the distributed ebbits infrastructure and the dynamic constellations of stakeholders require strict control of generation, distribution and usage of the data and strong security measures. Usage of data is also closely related to IPR management and economic business transactions. Moreover, the protection of data also involves ethical aspects and protection of personal data re the humans involved in the applications, such as those related to close monitoring of employees, etc. Data protection is a set of rules designed to ensure that the individual should have the possibility to control access to his or her personal information and to construct his or her own public persona. ebbits services should respect the data protection fair information principles.

[6] DG Information Society, Commission Factsheet 20, September 2004.

5. Product Liability

This section will undertake a brief review of some of the potential legal regimes for liability that may be relevant to alleged harms created by an ebbits like platform. The primary focus in this section will be the liability of an ebbit's system as a product, though it will also be looked at as a service when the laws of individual countries are discussed. The primary focus in the first part of this section will be on the European System of Product Liability introduced by directive 85/374/EEC.

This system is not comprehensive and is not capable of being applicable to all issues of liability in Europe, but it does represent largely the sole area where the liability of producers of products and services is harmonized across Europe. It thus represents an important first port of call for manufactures of products in Europe, given its application across all states of the European Union. Unfortunately a description of all other legal regimes that might also be applicable to liability issues in the ebbits project is far beyond the scope of this deliverable. The reader will however, in the second part of this section be presented with a description of the most relevant areas of law that are likely to be relevant in the Germany, Italy and the United Kingdom in order to paint a picture of the variability of law that can exist in terms of liability from state to state in Europe.

This deliverable, rather than representing a comprehensive legal opinion to the producer of an ebbits like system, represents an illustration of the potential issues that might be faced, and accordingly should be taken into account in production and deployment of such a system.

5.1 Product Liability – The Influence of Europe

Product liability arises through the idea that a consumer has a right to legal redress for damage that is caused by a defective product.[7] A ebbits system may be considered as both a product and/or a service depending upon the context where it is provided. Where an ebbits system has been fully delivered into the hands of another party and the ebbits producer retains no control over its operation, the producer of the ebbits system has effectively provided a product, which it has sold to the user. This may occur for example where an ebbits system has been installed into an automotive manufacturing factory, but it is the owner of the factory that takes control of the system thereafter. Where however the ebbits producer retains control over the product in question, e.g. maintaining and managing it, the ebbits producer will most likely be providing a service aimed at providing certain benefits e.g. energy efficiency, monitoring of food products etc.

The following pages discuss potential legal actions that arise in the first context (i.e. ebbits as a product). The laws applicable to ebbits as a service will be discussed later when looking at the law on liability on individual countries.

Traditionally redress for faulty products can be found through both contract and tort law. A solution in contract is often more difficult for a consumer that has been harmed to secure than is the case in tort. This is because for a consumer to have a valid action in contract for damage caused by a defective product, provision will usually have to exist in the contract allowing redress for such problems.[8] Consumers are also often in a position of greater weakness than sellers in terms of understanding and availability of information.[9] Often product suppliers or manufactures seek to leave such provisions out of contracts in order to reduce their own risks, weakening the protection for the consumer to be found in such contracts. In addition injured parties may on many occasions have no contractual relationship with the legal person that produced the goods in question. Such

[7] The concept of what product liability is can vary. In the UK it is taken to mean "that class of liabilities to which commercial manufacturers and commercial suppliers of goods are subject because a good has caused some form of actionable loss to either a business, a consumer or a bystander." See: Stapelton, J 'Product Liability in the United Kingdom: The Myths of Reform', (1999), *Texas International Law Journal*, 34, 45-70 See also: Clarke, Product Liability (Sweet and Maxwell. 1989). In the European Court of Justice case of Commission v France C-52/00 [2002] ECR I-3827 the court stated that where the PLD applies, old pre-existing systems can not longer apply. This means that in Systems such a s France and Germany, the previous systems that were more beneficial to consumers no longer apply.

[8] It should be noted however that in certain context certain implied terms can be created in contracts by statute. The Sale of Goods Act (1979) in the UK provides such an example.

[9] Stuart., C, (1981), "Consumer Protection in Markets with Informationally Weak Buyers", 12, 2, 562 - 573

issues associated with the law of contract often make it unappealing as a form of redress for harm caused by defective products.[10]

Fortunately, many legal systems have developed protection in their various systems of tort law. Such protection often appears in the form of a right of action for consumers who have suffered damage at the hands of various defective products against the manufacturer of the product in question, even if there is no direct relationship between the consumer and the manufacturer (i.e. the product has passed through the hands of intermediates).[11] In this way tort allows a flexibility that is often not present in contract law due to the notion of *privity* of contract[12].

5.1.1 Heterologous Legal Systems and Attempts at Harmonization

The varying situation with regard to tort systems in each Member State provided a cause for concern for the Commission because the presence of often differing and even conflicting laws represented a barrier to the implementation of the single market. In addition some Member States had particularly weak systems of tort law protection for those harmed by faulty products. These two issues posed two problems for the European Community in the 1980s. First, there existed greatly varying laws in each member state, creating problems for business certainty. Second, some states had weak systems of tort protection, leaving individuals that lived in those jurisdictions with limited protection.[13] As a result the Product Liability Directive (PLD)[14] was enacted.[15]

This directive harmonized (to a very limited extent) Member State tort laws by introducing a basic and uniform protection for consumers against defective products. The main principle of the directive is that consumers can hold manufacturers liable for defects in their products that give rise to damage. Where the principles of the PLD do not apply to a dispute, one must look to the various sources contained in national laws in order to discern the applicable law.

5.1.2 Why Might 85/374/EEC Apply to an ebbits Platform?

Defect is at the core of the PLD.[16] This contrasts with the notion of fault, which is at the core of many tort systems.[17] This is closer to a strict form of liability, as the claimant does not need to show that the manufacturer acted in an improper manner.[18] Although touted primarily as a measure taken to aid the protection of consumers[19] the PLD's regime also affects damage to professional users of products. The provision of services is not covered by the PLD. There is no European regime covering liability on the provision of services. National laws will therefore apply when such issues are in dispute. Primary agricultural products were originally exempt from the effects of the directive but this was later changed in a revision of the PLD.[20] This means that products such as cereals, cheese,

[10] Stanberry., B, (2006) "Legal and ethical aspects of telemedicine", Journal of Telemedicine and Telecare

[11] D*onoghue v Stevenson* [1932] UKHL 100 is the well-known decision from the House of Lords which established tort of negligence in the UK. There the court found that the manufacturer of a brand of ginger beer was ultimately responsible to the consumer who had become ill after drinking a bottle that was infested with snails. This was despite the fact that there was no direct relationship between the two as the beer had passed through middlemen in the meantime.

[12] The notion privity of contract expresses the idea that an individual that is not bound to a contract i.e a signatory cannot be bound by its contents. See: Lilienthal., J, (1887), 'Privity of Contract', Harvard Law Review, 1, 5, Dec 15, 1887

[13] Some systems such as France and Germany however had strong pre-existing systems of product liability. The imposition of the Product Liability Directive's regime has in such instance been seen to weaken protection and create a source of conflict between the new provisions and the ones that existed before. See: Fairgreave & Howells, 'Rethinking Product Liability: A Missing Element of the European Commission's Third Review of the European Product Liability Direcitve', (2007), *The Modern Law Review*, 70, 962-978

[14] Council Directive 85/374/EEC on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products. OJ L210/29

[15] An important motivator behind the directive, in addition to preventing competition distortions was the thalidomide disaster that occurred with children in the 1960s and 1970s. See: Stanberry., B, (2006) "Legal and ethical aspects of telemedicine", Journal of Telemedicine and Telecare, 12: 166-175, 174

[16] Fairgreave & Howells, 2007.

[17] This includes for example the UK's system of general negligence.

[18] European Commission 'Third report on the application of Council Directive on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products' COM(2006) 496 Final

[19] See for example Recital 2 of the Directive 85/37/EEC which speaks of apportioning a fair risk between the consumers and manufacturers of products.

[20] Directive 1999/34/EC extended the scope of Directive 85/374/EEC so that it now includes primary agricultural products (such as meat, cereals, fruit and vegetables) and game. See: A Guide to the EU Directive Concerning Liability for Defective Products (Product Liability Directive). (2001).

fish and meat are covered by the directive.[21] This situation was however changed with a revision to the directive made in 1999.[22] The primary reason for such a revision was the so-called 'mad cow disease' that was ravaging the agricultural sectors of several European Countries at that time, most notably, the UK.[23]

The PLD covers all 'moveable products', including software.[24] The PLD provides a system of liability for individuals that are harmed from products. This includes individuals acting in a commercial capacity and also individuals who have been damaged whilst acting as consumers. The PLD envisages liability for manufacturers where damage of the following type occurs.

Injury to Persons as a Result of a Defect in a Potential ebbits Platform

Injury to persons as a result of damage caused by a defect in the ebbits project will give rise to a cause of action under the PLD.[25] One can theorize that such injuries could occur to workers in the automotive manufacturing setting as a result of malfunctions in the operation of machines as a result of a defect in the ebbits system. In the context of agricultural production, injury as a result of a defective ebbits system is most likely to occur through the consumption of unfit food.

So-called 'emotional injuries' will not be governed by the PLD.[26] One could imagine such an issue arising for example where individuals eat meat products that, although not harmful, are not as they are so described e.g. not organic or halal. In such instances the psychological harm that may have been caused will not give rise to a claim under the PLD. Individuals will have to base any such claims on doctrines found in national law.

Where the PDL is applicable individuals will have to prove that there is a defect, in the ebbits system, and that such a defect caused the damage that has occurred to them.[27] In the case of injury that occurred as a result of plant machinery, individuals would be required to show that an injury that occurred was indeed caused by a defect in the ebbits system (e.g. a failure to anticipate a malfunction in plant machinery, or in the case of meat products, a mislabeling that leads to the consumption of harmful food).

Damage to Property as a Result of an ebbits Like System

Damage to private property can also be recovered under the PLD system.[28] Damage to property that is of a commercial nature is not however covered by the PLD. In both the automotive factory and the agricultural contexts, it is difficult to see how a defect in the ebbits system could result in damage to private property. Where a defect is likely to occur it is most likely to result in damage to property of a commercial nature, i.e. within an automotive factory or on an agricultural setting such as a farm. Even with the theorized used of an ebbits system in private homes to detect food that is out of date or counterfeit, it is difficult to imagine how a defect could result in damage occurring to private property. Where a defect does occur, damage, if it occurs, is likely to occur to physical persons (e.g. as a result of the consumption of effected meat.

The sole exception may be damage to the computer systems of the home that resulted as a result of installing the ebbits system at home e.g. the corruption of pre-existing programs or the accidental introduction of a virus.

[21] Id. at.

[22] These changes were made by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. Such changes were made as a response to the mad cow diseases crisis.

[23] See: Howells, *Product Liability - A History of Harmonisation*, *in* Towards a European Civil Code (A Hartkamp & E Hondius eds., 2004).

[24] In the original directive Article 2 defined products as "physical property and goods, as opposed to land or rights in or to real property. A product could include a whole product, part of another product, or part of a fixture attached to real property". *Directive 1999/34/EC* amended 85/374/EEC by redefining "product' as all movables even if incorporated into another movable or into an immovable. See : A Guide to the EU Directive Concerning Liability for Defective Products (Product Liability Directive) 2001 Available at http://gsi.nist.gov/global/docs/EUGuide_ProductLiability.pdf. See also Stanberry, *Legal and ethical aspects of telemedicine*, *in* Introduction to Telemedicine (V Wooten, et al. eds., 2006).

[25] See Article 9

[26] Article 9(a) forsees only claims for "death or by personal injuries"

[27] Article 4

[28] Article 9(b)(i)

5.1.3 Where 85/374/EEC may NOT apply to an ebbits Platform

The PLD is not applicable to liability issues arising from certain types of damage as a result of a product defect. Where this is the case it does not mean that no liability exists, but only that it does not exist under the PLD. Other forms of liability e.g contractual or non-contractual (tort) are likely to exist in national legal systems. Given that the PLD is the sole instance of harmonization in such issues of liability law, this means that the existence of liability and how it is treated will vary from one Member State to the next. Examples will be shown the second part of this section to demonstrate this from United Kingdom, Germany, and Italy. The most important instances where the PLD will not be applicable to damage relating to a defect in a potential ebbits system are:

Damage To Commercial Property

In the other cases where damage resulting from a defect occurs to commercial property recourse will have to be found in alternative systems of liability based in national law. Such a situation could be for example envisaged in the automotive context where machinery is damaged or in the agricultural production context where live stock is harmed.

Economic Losses i.e. not physical losses

The PLD does not allow individuals to recover for purely economic losses. These are the types of losses that are most likely to occur should there be a defect in the ebbits system. This could occur in the automotive manufacturing context for example where a defective ebbits system led to an higher than expected level of energy consumption in the manufacturing cycle, with the consequences that costs for the manufacturer where higher. The same would apply where such overuse led to contract violations - connected perhaps to guaranties for the low energy production of vehicles. In the agricultural context, a mislabeling of meat produce may lead to economic loss due to wasted meat, or perhaps in the form of damaged business relations between various elements in the chain from farmers through slaughter houses through suppliers and finally to the consumer. Such loss of trust could result in loss of business and or future contracts, leading to economic losses. Such losses are not recoverable under the PLD. Individuals or businesses whishing to recover such losses will have to seek remedies in national law (i.e. not outlined within the PLD) where they exist.[29] Given the potential variation in such laws from state to state, it is not possible to describe them in detail in this document.[30]

5.1.4 What Constitutes a Defective Product under 85/374/EEC?

A product is not simply defective because it has caused damage. Many products can cause damage if they are not used in a correct manner. Using a paperclip as a temporary replacement in a complex industrial machine is likely to lead to problems and potential damage when the machine inevitably malfunctions. This does not mean that the paper clip itself was however 'defective'. No manufacturer or user of a paper clip would reasonably expect that it could effectively be put to such a use. The PLD reflects such an intuitive concept in its description of what would constitute a defect. It states that a product is defective when it "does not provide the safety which a person is entitled to expect, taking all circumstances into account".[31] In deciding what a user of the product in question should expect, the directive states one should take into account the uses it could reasonable be put to,[32] the presentation[33] of the product and also the time when it was put into circulation.[34]

The factors described here will be important in deciding whether any damage that has been caused by an ebbits like system can be claimed to be caused by a 'defect' and thus give rise to potential damages. In terms of expected use, it is reasonable to expect, that any particular ebbits like system will be designed for a very specific use.

[29] It is often difficult to mount non-contractual (tort claims) for pure economic loss in man legal systems. This can be seen for example in the tort systems of the UK and Germany. See part 2 of this section for more detail.

[30] See however part 2 of this section for a brief description of some applicable laws in Germany Italy and the UK.

[31] Article 6(1)

[32] Article 6(1)(b)

[33] Article 6(1)(a)

[34] Article 6(1)(c)

A key factor for a manufacturer in avoiding potential liability is the adequate representation of risk with the product in its presentation. This will be especially important in the consumer context where individuals will perhaps have different and sometimes unrealistic expectations concerning potential risk than a commercial purchaser might. It is therefore important to appraise the purchaser of a product in an honest manner about the risks of defect for a given product. This will allow consumers to take adequate precautions when handling the product in question.

In the potential agricultural context this may involve warning consumers that use ebbits RIFDs that errors in meat production can occasional occur. A potential strategy may be to inform end customers (possibly through disclaimers that appear on their smartphone when scanning a product) that the information that they have been provided is to be viewed as an aid to judging quality and not a guarantor of the safety of the meat. Customers should accordingly be informed that the risk involved in eating such meat are the same as for eating other meat that is not followed by an ebbits like system. Such warning will avoid giving potential consumers of the ebbits controlled meat a false perception that it is 100% safe.

In the automotive context packaging as understood in the consumer context is less likely to be an important issue. An ebbits like system installed in an automotive context is unlikely to come packaged in such a simple manner with a set of simple instructions designed for consumers. In the automotive manufacturing context, for reasons explained above, the only liability likely to face the producer of an ebbits system through a defect is likely to be where such a defect has resulted in the injury of a worker working on the production line.[35] In order to avoid such liability it will be important to relay to those working on the system accurate information concerning the potential chance of a defect and the potential consequences (if they exist in terms of personal injury). One possibility is to require (potentially in contracts agreed with automotive manufactures) that those who work on ebbits controlled machinery are informed with suitable (possible reading or video) material of the risk of defect in the ebbits system.

5.2 Potential Defences Available to Manufacturers

5.2.1 A Suppliers Defense

The original directive allowed suppliers to avoid liability if they were able to identify the manufacturer of the product in question.[36] The apparent intention of the drafters of the directive had seemingly been to create a regime that was primarily concerned with those who manufactured products and not those who supplied them.[37]

The availability of this defense can act as an important reassurance for suppliers, that at least from the perspective of the PLD, they will be able to avoid liability for a product they have supplied, if they can identify the actual manufacture or producer who was responsible for the fault. In the context of a potential ebbits platform this may act as an important element of reassurance for potential suppliers when deciding to work with products that may use such a system. In the agricultural supply context for example, vendors such as supermarkets, will be able to know that if damage occurs to individuals consuming meat products, as result of a defect in the ebbits system, they will be able to shield themselves from liability by identifying the ebbits manufacturer as the party that should be held liable. Such a situation has obvious positive and negative aspects. In terms of positive aspects it means that potential partners such as suppliers and vendors will not be

[35] An ebbits manufacturer may however face claims concerning damage to commercial property or economic losses under alternative legal regimes based in national law. These may for example include negligence based claims for damage to commercial property or contract based claims for economic losses.

[36] Article 3(1) that: '"Producer" means the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part and any person who, by putting his name, trade mark or other distinguishing feature on the product presents himself as its producer.'

[37] However, point 2 of the minutes of the meeting of the Council of Ministers
of 25 July 1985 stated: "With regard to the interpretation of Articles [3] and [13], the Council and the Commission are in agreement that there is nothing to prevent individual Member States from laying down in their national legislation rules regarding liability for intermediaries, since intermediary liability is not covered by the Directive. There is further agreement that under the Directive the Member States may determine rules on the final mutual apportionment of liability among several liable producers" Quote taken from Fairgreave & Howells, 2007. P 975

'frightened off' from supplying and selling meat products that rely on an ebbits system for their verification. The negative aspect of the 'suppliers defence' however is that, where damage does occur as a result of a defect in the ebbits system, intermediate suppliers will likely do their utmost to point the finger in the direction of the producer of the ebbits system.

5.2.2 Non-liability Due to the Non-Discoverability of the Defect in Question

In its proposal for the directive, the EU Commission wanted the directive to provide for a regime of strict liability, something that was new to some Member State legal systems.[38] The UK for example had a system of liability based on the doctrine of negligence and the concept of "reasonable foreseeability". The proposed new system of strict liability would mean that manufactures would be responsible for all defects (that caused damage) to their products even if they had not been at fault in their design or manufacture. In the negotiations concerning the directive however, it was impossible to achieve agreement of such a broad form of liability of manufactures.[39] There are therefore a number of defenses available in order to avoid an absolute form of strict liability.[40] The most contentious of these potential defenses and likely the most important from the point of view of the ebbits platform is the defense of 'non-discoverability'. This defense allows the producer of a system such as ebbits to avoid liability for defects in its product if "the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered".[41]

This concept envisages a wider range of possible liability than that which was for example the case under UK law, whereby a defect had to be 'reasonably foreseeable' to exist. The concept of 'discoverability' means that a manufacturer can be held liable where one could have discovered the fault in question, even where it was not reasonable to do so i.e. it was extremely difficult. The directive's reference to 'available scientific' and technical knowledge however narrows the range of potential liability slightly, in that the defect in question must have been discoverable using the contemporaneous knowledge available at the time of production. This means for example experimental data that is available to others but which has not yet been published will not be considered as being available to the manufacturer in question. It is therefore of crucial importance for manufacturers to be aware of the current state of knowledge, especially in the scientific literature at the time of manufacture. Cases that involve harmful defects may revolve around the scientific and other related literature available at the time of manufacturer to see if the manufacturer involved could have discovered the fault in question. This means that a comprehensive review of the scientific and other literature is indispensible to manufacturers in order to prevent 'discoverable defects' being integrated into the product. This should be conducted before the creation of products that are likely to be put on the market and should continue until the product has been placed on the market. Such a review must indeed be comprehensive for some judges in certain cases have made comments hinting that published knowledge anywhere in any language will be taken into account when deciding what was discoverable.[42] In order to do this manufacturers are required to have documentary evidence that any damage that might arise was undiscoverable at the time of manufacture.[43] Producers of an ebbits system must therefore show that they had an up-to-date knowledge of the literature and findings on relevant issues in the event of defects arising.

[38] The UK for example did not recognise a system of strict product liability before the directive was created.

[39] Some states such as the UK feared that such a broad form of strict liability would result in too much harm to the interests of manufacturers. See: Stapelton, 1999.

[40] The others are more general and relate to individuals who want to deny that they are indeed the manufacturer of the product in question. Those relate to producers that can show that Article 7(a) that he did not put the product into circulation; or (b) that, having regard to the circumstances, it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him or that this defect came into being afterwards; or (c) that the product was neither manufactured by him for sale or any form of distribution for economic purpose nor manufactured or distributed by him in the course of his business; or (d) that the defect is due to compliance of the product with mandatory regulations issued by the public authorities; or (f) in the case of a manufacturer of a component, that the defect is attributable to the design of the product in which the component has been fitted or to the instructions given by the manufacturer of the product.

[41] Article 7(e)

[42] Howells, 2004 P653. See also comments by Mr Justice Burton on the applicability of results published only in Manchuria (a humorous analogy) in English *National Blood* case [2001] 3 All ER 289.

[43] Directive 85/374/EEC, Article 7(e)

5.3 Other Systems of Liability Permitted Under 85/374/EEC

The European Court of Justice (the ECJ) has described the PLD as an instrument of maximum harmonization. This produced some confusion with some arguing that the directive precludes other forms of liability for defective products.[44] This has not however been accepted by most European jurisdictions where alternative systems have persisted. The prevailing wisdom seems to be that whilst Directive 85/374/EEC precludes other systems of liability based on the concept of 'defect', it does not affect alternative systems of liability based on concepts such as 'negligence'.[45] As a consequence, where the provisions do not apply, there are often other laws, depending on the particular Member State in question that can be invoked. Unfortunately these laws vary considerably from state to state. As a consequence it is not possible to describe the varying situation for each state in the EU. In order to keep the content of this deliverable manageable this section will present a brief overview of the most relevant systems of law in the United Kingdom, Germany, and Italy.

5.3.1 The United Kingdom

The PLD was implemented in the UK[46] by the Consumer Protection Act 1987. Before its implementation the main pillars of law applicable in defective products were the system of 'Statutory Warranties' as laid down in the Sale of Goods Act 1979 and the tort of negligence as provided for in the common law.[47]

The latter also has relevance for the provision of services in the UK. These legal systems will be described below.

Contract Law/Sale of Goods

Contract law in the UK is similar to that which exists in most Common Law jurisdictions. Two important characteristics that are strongly emphasized in English and Welsh contract law are the concepts of 'consideration' and 'privity'. The notion of 'privity' is important as it means that only parties to the contract in question have a right to damages in the event of a breach of contract. From the perspective of the ebbits project, this is relevant because it means that under UK law only a party that had concluded a contract with the ebbits producer could claim damages under contract law in the event of damages caused by a faulty product. This means that ebbits will not be liable to third parties under provisions under contract law, unless provisions within the contract in question so specify (see the discussion on the the Contracts (Rights of Third Parties) Act 1999 below). This will be important in both the automotive manufacturing context and the agricultural production contest, especially where the damage is only of a purely economic nature (see below).

The Sale of Goods Act in the UK creates 'statutory warranties', which are in reality statutorily mandated terms that are taken to exist in contracts for the sale of goods. The act therefore creates certain obligations on the part of the seller of goods that have to be met, even if not specifically described in the contract.[48] Such guarantees are available to commercial and non-commercial buyer alike.[49] Such guarantees relate *inter alia* to 'product quality' and 'fitness for purpose'. In deciding whether such guarantees have been taken into account use can be made of the information provided with the product including the instructions.

Unlike the liabilities created by the PLD, the liabilities created by the statutory guarantees contained in the Sale of Goods Act also allows a party that is harmed to recover for pure economic loss.[50] This

[44] Fairgreave & Howells, 2007. P976

[45] The notion of defect as described in Directive 85/374/EEC does involve the concept of reasonableness, an important concept in negligence law in the UK for example.

[46] The reader wishing to acquire an indepth knowledge of UK law on such matters should consult *J. P. Benjamin*, Sale of Goods, 6th ed. 2002; *J. Chitty*, On Contracts, 28th ed. 1999; *J. F. Clerk/W. H. B. Lindsell* on Torts, 18th ed. 2000; *J. Cooke/D. Oughton*, The Common Law of Obligations, 3rd ed. 2000; *C. Cross/S. Bailey*, Cross on Local Government Law, 1986; *A. M. Dugdale/K. M. Stanton*, Professional Negligence, 3rd ed. 1998; *R. M. Jackson/J. L. Powell* on Professional Negligence, 4th ed.1997; *J. McEldowney*, Electricity Industry Handbook: Law and Practice, 1992. Quoted in Comparative Analaysis of National Liability Systems for Remedying Damage Caused by Defective Consumer Services - A Sudy Commisioned by the European Commision. (2004).

[47] Stapelton, 1999. P48

[48] Such contract sneed not be written and can be implyed through oral agreement.

[49] Stapelton, 1999. P48

[50] Atiyah, P, 'The Sale of Goods. (9th ed, 1995) See Chapter 20.

is typical of contract law in the UK in general, which unlike the law governing non-contractual liabilities allows for recovery of purely economic losses. From the point of view of a potential ebbits platform the possibility of claiming compensation for pure economic loss is important. In the automotive manufacturing context, such losses may arise where energy consumption is higher than expected. In the agricultural food production, such losses may occur where reliability issues harm the reputation of certain food producers or vendors, resulting in reduced sales i.e. economic loss. Where a relationship of a contractual nature exists between the producer of an ebbits platform and such parties, the producer will be liable for such economic losses where the ebbits platform does not perform as specified in the contract (either explicitly or implicitly through statutory provisions such as the Sale of Goods Act). Where the ebbits producer has a direct contractual relationship with the party that suffered the loss in question it may be liable for such losses if they arose as a result of a defect in 'the ebbits system.'

Such a relationship may exist in the automotive manufacturing setting where the ebbits system is provided directly an installed by the producer. It may exist in the agricultural production context where the ebbits producer has a direct contractual relationship with farmers, suppliers or vendors etc. Where the ebbits system has been supplied and installed by an intermediate party (i.e. where a contractual relationship only exists between such parties) such liability will not exist. It should be noted however that the notion of privity was softened in UK contract law with the introduction of the Contracts (Rights of Third Parties) Act 1999. This law allows obligations for third parties to be created (who are not part of the contract) if the contract so specifies. This means that the producer of an ebbits platform could be liable under contractual law for harm caused to third parties (including economic losses), but only if so agreed in the contracts it signed. This could be relevant in contracts signed between the producer of the ebbits system and intermediaries e.g a supplier that installs the system in automotive manufacturing sites or, in the agricultural production context farmers, suppliers or vendors of food. In such cases care should be taken in the chosen contractual provisions in order to minimize liabilities.

Negligence

The tort of negligence[51] entitles any party to recover damages where another party has acted in a negligent way that caused physical harm or damage to private or commercial property contrary to the 'duty of care' he owes the party in question.[52] Such a relationship means that the concept of privity does not exist in the doctrine of negligence. This means that a producer of a product can be held liable, even where there is no contractual relationship between the two. There does however have to be a relationship known as a duty of care. Such a relationship exists between manufacturer and the final consumer of the product (even where no direct contractual relationship exists). The producer of an ebbits system could thus be liable where its product caused harm to individuals or the property of end consumers.

Unlike the PLD which operates at the European level, such harm also includes damage to commercial property. This means for example that in the automotive manufacturing context, a manufacturing plant may be able to claim for damage caused by an ebbits platform, even where there was no direct contractual relationship between the two (this might for example exist where an ebbits system was sold and installed by an intermediary). The doctrine of negligence in England and Wales does not however in most circumstances cover pure economic losses. This means that in the automotive manufacturing sector for example, a car manufacturer would unlikely be able to make claims under the doctrine of negligence for unexpected economic costs (e.g. increased energy use) that would arise from a fault with the ebbits system. Normally such losses could only be recovered where a contractual relationship exists, under contract law as described above. Another aspect that separates the doctrine of negligence from the system outlined in the PLD above is that it revolves around a finding of 'negligence' and not simply a 'defect'. This means that even where a defect exists, an manufacturer may escape liability if the claimant can not prove that the manufacturer was negligent, i.e. that they could not have reasonably have been expected to prevent it. This is a less onerous standard than the concept of 'discoverability' outlined in the PLD. As with the PLD,

[51] The seminal case for the doctrine of negligence in the UK was Donoghue v Stevenson 132 APP Case 562. The case concered the supply of a bottle of beer that was found to have a snail in it. The court allowed the claimant to claim damages, despite the fact that there was no contractual relationship between the two.
[52] Stapelton, 1999.

claimants must also demonstrate that damage was caused by the negligence of the party concerned and that damage was caused as a result of such negligence.

Liability for Services

Liability for faulty Services in the UK usually exists through contract law. A contractual relationship must therefore exist between the two. Most of the law concerning such relationships is common law, i.e. created through precedent, though there are some important statutory interventions. The Supply of Goods and Services Act 1982 contains a general provision which applies to most contracts for services and requires the service provider to exercise reasonable care and skill when providing the service. For potential large commercial contracts (as would likely exist for the supply of an ebbits like platform), the relevance of such implied terms is limited as one would expect that such terms would be explicitly included in contracts of large economic value that are properly drafted. Such terms creates duty of care equivalent to that which exists under the concept of negligence described above.[53] For liability to exist for contracts for services the claimant must show the service provider has violated the duty to act with reasonable care and skill and has neglected the ordinary standard of professional diligence.[54]

5.3.2 Germany

In Germany[55] the main legislation controlling both contractual and tortious liability are contained in the Civil Code or *Bürgerliches Gesetzbuch* (BGB). This was created in 1900 and has been modified until the present day.[56] Although the role of precedent is less important in the German system than in common law systems such as the UK, previous judgments by the court do play an important role in interpreting the law. As in the UK, a wider range of liabilities exist where there is a contractual relationship between the parties in dispute. The Gesetz zur Modernisierung des Schuldrechts[57] however lessened this difference, providing for extra rights in terms of non-contractual liability, especially for consumers.[58] The most important aspects of these laws are described briefly below. In Germany the main provisions of Council Directive 85/374/EEC on Product Liability were implemented by the Produkthaftungsgesetz vom 15. Dezember 1989 (BGBl. I S. 2198). This transposed the principals of the EU Product Liability Directive as discussed above into German law. The paragraphs below will discuss some idiosyncratic aspects of German law relating to contractual and non-contractual liability.

Contractual Liability

Damages are available under German law where parties have failed to perform their duties as specified in the contract with the consequence that damage has occurred.[59] Unlike the law in the UK, German law also requires that the defendant party have been negligent in his actions. This provides an extra defense for contracting parties, not available under English law. This reflects the concept in German contract law that a defendant is only "obliged to act with reasonable care but cannot, and cannot be expected to, guarantee the result."[60] In the context of the ebbits platform this could provide a useful protection in the automotive manufacturing context if for example a manufacturer claimed that the energy savings had not been what it had expected under the contract in question. In such an instance an ebbits producer would be able to escape liability if it could show that it had acted reasonably in order to meet its contractual obligations. This might for example be shown by

[53] See s13 Supply of Goods and Services Act 1982.

[54] Comparative Analaysis of National Liability Systems for Remedying Damage Caused by Defective Consumer Services - A Sudy Commisioned by the European Commision 2004 P106

[55] For a comprhensive pciture of German law in this area the reader can consult *W. Erman* (ed.), Bürgerliches Gesetzbuch, 10th ed. 2000; *O. Jauernig* (ed.), Bürgerliches Gesetzbuch. Kommentar, 10th ed. 2003; *H. Kötz/G. Wagner*, Deliktsrecht, 9th ed. 2001; *H. Lange/G. Schiemann*, Schadensersatz, 3rd ed. 2003; *D. Medicus*, Bürgerliches Recht, 19th ed. 2002; *Münchener Kommentar zum Bürgerlichen Gesetzbuch*, 3rd/4th ed. 1997 ss; *O. Palandt* (ed.), Bürgerliches Recht, 62n ed. 2003; *R. Zöller* (ed.), Zivilprozessordnung, 22nd ed. 2001. Quoted in id. at.

[56] Id. at. P52

[57] vom 26. November 2001 (BGB1. I Seite 3138)

[58] Schuldrechtsmodernisierungsgesetz, 26. Nov 2001 (BGBl. 2001 I 3138).

[59] Under German law the term for not fulfilling his/her duties as a vendor (or maybe producer) is Pflichtverletzung. The vendor is obliged to offer his product free of material defects and defect of title

[60] Comparative Analaysis of National Liability Systems for Remedying Damage Caused by Defective Consumer Services - A Study Commisioned by the European Commision 2004

reference to accepted good practice and standards. German contract law also recognizes the notion of good faith. Where breach of contract has been alleged, the burden of proof rests on the party that alleges to have been harmed. Claimants are also required to prove that where damage occurred, it was the result of a breach of contract. This would mean that if running costs in the automotive context were higher, a claimant manufacturer would have to prove that this was a result of a failure in the ebbits system.

The notion of privity in German contract law is much weaker than in UK law. This means that contracts can provide protection for third parties. Unlike the UK this can occur both where the contracting parties have so specified and where they have not.[61] Courts will be willing to impute such obligations where it is obvious that certain individuals by close connection to the contract in question depend on performance of the contract and would be left without a remedy if such a duty was not inferred.[62] This could be of relevance for the potential agricultural food production context of the ebbits platform. This is because end consumers (and perhaps suppliers and vendors too) might suffer damage through a defect in the ebbits system. Under German contract law, such individual may have a right of action against the producer even though there was no contract between the parties, by virtue of the contractual obligations of the ebbits producer to other parties e.g. to famers or other agricultural producers.

Non-Contractual Liability (Tort)

Non contractual liability in Germany is of a different nature than most other jurisdictions including those both in civil law and common law legal systems. Unlike the situation in say France or the UK where the liability in negligence is described in terms of a relatively simple formulation that can be applied to many types of harm and context (e.g. negligence in the English and Welsh common law)[63], German law has chosen to opt for a more methodological form. Rather than a general duty, Germany law recognizes liabilities where a protected interest of individuals is harmed by another.[64] The most famous of these allows recovery of damages for "harms to life, body, freedom, property or 'other rights'".[65] The term 'other right', might be appear very expansive at first glance, allowing potentially for the recovery of a number of other harmed interests, including pure economic loss.[66]

This is, however, not the case with section 823 BGB being interpreted as not covering economic losses. Such losses are rather covered by Section 826 BGB of the civil code that describes a persons 'wealth' as a protected interest. The scope of this article is however limited though to situations where the harm caused is 'willful'. This means that errors or faults that are merely careless will not be sufficient to engage this article, with the result that pure economic loss is not recoverable for acts that are simply negligent.[67] As a result, pure economic loss in Germany is only protected for in exceptional circumstances, e.g. where there was 'willful wrong doing'.[68] This means that for the ebbits project, it is unlikely that claims for pure economic loss will be made against a producer of the system under German tort law. This is because the requirement of willful wrong doing is not likely to occur. Where a fault did cause harm resulting in pure economic loss to a legal individual, such events are likely to have not been caused intentionally by the ebbits producer. If such faults were the result of an accident, or even negligent behavior, Article 826 BGB (relating to pure economic loss) will not be engaged. This could be important in both the automotive manufacturing and agricultural production settings for a possible ebbits platform. In the former pure economic loss might result from higher than expected energy costs. In the latter such loss might result where a defective ebbits product caused reputational harms resulting in lost sales e.g. for suppliers and

[61] See cases Erman-*H. P. Westermann*, § 328 no. 11 ss; Palandt-*H. Heinrichs*, § 328 no. 13 ss.

[62] See *Bürgerliches Gesetzbuch Section 278*

[63] The Classic formulation for negligence under English and Welsh Common law is that a legal person is labile where his actions have resulted in damage to another party to whom he owed a duty of care. This formulation was laid down in the seminal case of UK was Donoghue v Stevenson 132 APP Case 562

[64] These interests are found in the German civil code, i.e., BGB s823-853.

[65] Spindler & Rieckers, Tort Law in Germany § London (Kluwer Internaitonal. 2011). P 39

[66] It includes for example copyright, patent law, family interests e.g. relationships etc. See id. at.

[67] Translated by BASIL S. MARKESINIS, THE GERMAN LAW OF TORTS 14 (4th ed.
2002). Mauro Bussani & Vernon Valentin Palmer, *The liability regimes of Europe—their facades and interiors*, *in* PURE ECONOMIC LOSS IN EUROPE, *supra* note 6, at 120, 148; Erwin Deutsch, *Der Ersatz reiner Vermögensschäden nach deutschem Recht*, *in* CIVIL LIABILITY FOR PURE ECONOMIC LOSS, *supra* note 6, at 55; Mathias Reimann, *Case 3:cable III—the day-to-day workers*, *in* PURE ECONOMIC LOSS IN EUROPE, *supra* note 6, at 218.

[68] Koziol, 'Recovery for Economic Losses in The European Union', (2006), *Arizona Law Review*, 48, 871-895

vendors. Where legal individuals in such circumstances do wish to recover purely economic losses they will only be able to do so through contract law (unless they can show willful intention), if the contractual provisions that have been agreed allow them to so do.

In contrast to claims for pure economic loss, claims under s 823 BGB do not have to be willful. Awards under German tort law under s 823 can also be made without the need to establish a duty of care or fault, if the claimant can show that the defendant's actions were responsible for the damage in question. Such liabilities are therefore much more 'strict' in Germany than in the UK where there is a need to show a 'duty of care relationship and that the defendant was negligent i.e., that he did not act according to a 'reasonable' standard. This means that where personal injury was to occur e.g. in the automotive manufacturing context, claimants will find it relatively easy to show liability if it can be shown that the ebbits platform was at fault. This is in comparison to the UK for example where negligence must be shown.

Until relatively recently the law had remained relatively unchanged from its codification in the early part of the 20th century. A series of cases had exposed the existing codification of tort law as missing a number of important elements. As a result a revision was made to several important areas.[69] One important area was to allow claims for 'immaterial loss'. Such loses cover a number of areas that might be of relevance to the ebbits project. This includes the possibility of claims for emotional injury.[70] This could for example conceivably occur in the agricultural production context where through errors in food labeling individuals consume products that they would not want to. This could be for example where meat was not halal, not organic, not ethically produced etc.

5.3.3 Italy

In Italy[71], there is a double track protection in the area of product liability. Plaintiffs can sue under both the Consumer's Code, Part IV, which incorporates the no-fault principle of the EU's Product Liability Directive (85/374/EC), and also under article 2043 of the Italian Civil Code, according to which the plaintiff must prove the defendant's negligence or fault.

Article 2043 Italian Civil Code: Tort Liability

Article 2043 of the Italian Civil Code enshrines the legal principle of 'neminem laedere' (hurt no one) in civil matters. It states that: ' Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno' (article 2043 Risarcimento per fatto illecito, = tort). This lapidary formulation provides that 'any person who by willful or negligent conduct causes unfair detriment to another party must compensate that injured party for any resulting damage'.

Article 2043 ICC allows individuals to sue manufacturers for damage caused by defective products. In general, under Article 2043 ICC, the plaintiff must prove:

- The defect of the product;
- The damage suffered;
- That the product defect caused the damage; and

[69] The Reform of German Tort Law. (2003).

[70] s253(2) of the BGB states that "injury of body, health, freedom and sexual self-determination" can give rise to liabilities. Translation taken from id. at.

[71] The reader wishing to acquire an indepth knowledge of Italian law on such matters should consult G. Alpa, Il problema dell'atipicità dell'illecito, 1979; G. Alpa/M. Bessone, I fatti illeciti, Trattato di diritto privato diretto da Rescigno, XIV, 1982; C. M. Bianca, Diritto civile, 3, Il contratto,2000; id., Diritto civile, 5, La responsabilità, 1994; id., Diritto civile, 4, L'obbligazione, 1990; morale, in Digesto delle discipline privatistiche, Sez. civile, V, 1989, 83; F. D. Busnelli, La lesione del credito da parte di terzi, 1964; C. Castronovo, La nuova responsabilità civile, 2a ed., 1997; P. Cendon/F. Ziviz (a cura di), Il danno esistenziale, 2000; G. Cian, Antigiuridicità e colpevolezza, 1966; M. Comporti, Esposizione al pericolo e responsabilità civile, 1965; A. De Cupis, Dei fatti illeciti, in:Commentario al codice civile a cura di Scialoja e Branca, 2a ed., 1971; F. Realmonte, Il problema del rapporto di causalità nel risarcimento del danno, 1967; C. Salvi, La responsabilità civile, in Trattato di diritto privato a cura di Iudica e Zatti, 1998; G. Visintini, Inadempimento e mora del debitore, in: Il Codice Civile. Commentario diretto da P.Schlesinger, 1987. These and otehr sources are drawn from *Comparative Analaysis of National Liability Systems for Remedying Damage Caused by Defective Consumer Services* - A Sudy Commisioned by the European Commision. (2004).,p.65. This section draws from internet sources, in particular Marco Lombardi and Giulio Novellini. (2012). Product Liability Law In Italy, Mondaq Business Briefing - Jones Day, http://vlex.it/vid/product-liability-law-in-italy-408895054.

- The defendant's negligence or fault.

Negligence is typically an element necessary to establish liability. However, some court decisions and legal scholars sustain that, further to the transposition in the Italian legal order of the EU PLD (discussed below), the defective nature of a product alone is sufficient to prove negligence in the manufacturing process. More explicitly, it is suggested that the manufacturer's fault can be proved by the mere existence of the defect generating the damage (no fault liability).

Claims brought under Article 2043 ICC are subject to the general five-year tort liability limitation period, starting from the time when the claimant could exercise his or her rights. The time limit is extended if the tort is connected to the perpetration of a crime. Moreover, when the damage is of a continuing nature or is aggravated over time, the limitation period starts from the aggravation that gave standing to sue. In addition, moral damage ('danno morale)[72] can also be compensated.

The Consumer's Code – Legislative Decree No. 206/2005

As mentioned earlier, article 2043 ICC coexists with the strict liability system governed by the Consumer's Code (Legislative Decree No. 206/2005), which transposes the EU Product Liability Directive (85/374/EC) into the Italian legal order (originally implemented by Legislative Decree No. 224/1998, as mentioned above).

The Consumer's Code harmonises the level of protection of consumers and users in accordance with the principles of the European Union's legislation. In force since 23 October 2005, it provides rules designed to protect consumers: transparency in banking and consumer credit agreements, regulation of contracts and liability of financial brokers, insurance contracts, and regulation of the retail trade fall within its purview, in conjunction with other laws (including the ICC). More specifically, the Code :

a) Recognises the fundamental rights of users and consumers to health, safety, information, correctness in advertising, consumer awareness and education, and propriety and fairness in contracts;

b) Regulates some aspects of consumer contracts, including warranties applicable to the sale of consumer goods and post-sale duties;

c) Addresses consumer access to justice and the form of collective actions;

d) Regulates product safety and product liability.

With respect to product liability (d), the Consumer's Code, Pat IV, brings Italian law in line with the Product Liability Directive 85/374/EC. Reflecting the provisions of the PLD, the Consumer's Code defines "product," "defective product," "manufacturer," "supplier," and the scope of manufacturers' and suppliers' liability. Article 117 of the Code provides that a product is defective when it does not provide the safety that one can reasonably expect, taking all circumstances into account. These circumstances have been addressed earlier in this paper and they include: packaging, evident features, instructions, warnings supplied, the product's reasonably expected use and life cycle, and the period during which the product was distributed.

Seen from the viewpoint of the injured party, in product liability claims under the Consumer's Code, the injured party must provide evidence of:

- The product defect under the Consumer's Code definition;
- The damage incurred (based upon general tort rules);
- The causal relationship between defect and damage (on the basis of the general principles of causation in tort laws, proof of causation is often achieved through presumptions).

Importantly, and unlike under article 2043 ICC, no evidence of fault is required. This means that the injured party must prove the damage, the defect in the product, and the related causation, but not the manufacturer's fault. Since the plaintiff has no burden of proving fault, the burden of proof falls

[72] *Danno morale* is commonly used to designate and describe every damage inflicted upon interests that are not considered patrimonial, such as mental anguish, humiliation, and emotional distress.

on the defendant's shoulder, who must provide evidence excluding liability (e.g., proving the plaintiff used the product inappropriately).

Possible conflict between EU product liability regime and the Italian Civil Code's rules on tortious liabilities

With decision No. 13432/2010, the Italian Supreme Court (*Corte di Cassazione*) confirmed the double-track protection system, based on both the EU's product liability regime and domestic rules on tortious liabilities. In this decision, which concerned a case about damage caused by a defective car, the Supreme Court ruled that product liability claims can be grounded in the tort rules based on fault or negligence set out in Article 2043 ICC, *in addition to* the strict-liability regime under the Product Liability Directive. The Supreme court justified this decision arguing that 'the national legislature, giving effect to the EU Directive, intended to give broader protection to the consumer, […] as anchored to the evidentiary burden imposed by the rules on liability in tort pursuant to art. 2043 [of the Italian Civil Code]'.[73]

The 'evidentiary burden' is at the center of the double-track protection system, and it concerns the consumer's compensation for damage, i.e., nonmaterial or moral damage, that is not expressly provided for in the EU PLD and in article 123 of the Consumer's Code, which transposes it.[74] In a 2003 judgment regarding personal injuries caused by a defective ladder[75], the Milan District Court denied recoverability of moral damages in strict liability-based cases are twofold. The court pointed out that the strict liability regime does not provide explicitly for the recoverability of moral damages. Indeed, under article 9 of Directive 85/374, the term 'damage' does not include non-material damage.[76] The same provision is transposed in Italian law by Law 224/88 (article 11), subsequently repealed by Dlgs. 206/05 (Consumer's Code) (article 123). Conversely, under Article 2059 of the Italian Civil Code, moral damages are recoverable, but the negligence of the conduct must be proved. Courts have objected to the application of this norm to a strict liability-based claim. Therefore, they have tended to resort to Article 2059 of the Civil Code to compensate moral damages, balancing this with the lack of provisions in the EU liability no fault regime incorporated in the Consumer's Code.

The possibility to sue for moral damages, which is not foreseen under the strict liability regime flowing from EU law, seems to be the only element justifying the double-track protection system for injuries caused by a defect in a product. As discussed earlier, the European legislature wanted to promote harmonisation with regards to product liability rules. However, article 13 of the EU Product Liability Directive permits cumulative theories of liability.[77] Similarly, article 9, which defines 'damage', explicitly states that 'this Article shall be without prejudice to national provisions relating to non-material damage'. In the case *Moteurs Leroy Somer v Dalkia France and Ace Europe* of 2009[78], the European Court of Justice confirmed the legitimacy of the double track system of protection. The Luxembourg court interpreted article 13 of the Product Liability Directive as meaning that 'the system of rules put in place by the directive does not preclude the application of other

[73] Ibid. '*In particolare il legislatore nazionale, dando attuazione alla direttiva comunitaria, ha inteso accordare una tutela più ampia al consumatore, superando i rigorosi limiti che in precedenza essa incontrava sia nell'ambito del rapporto con il venditore, in considerazione della contenuta azionabilità nel tempo dei diritti di garanzia riconosciuti dalla disciplina ordinaria della vendita, sia al di fuori del rapporto negoziale, in quanto ancorata agli oneri probatori imposti dalle regole in tema di responsabilità aquiliana ex art. 2043 c.c'*

[74] Article 123 of the Consumer's Code provides for the refund to the consumer of only: (i) damages resulting from death or personal injury caused by a defective product; or (ii) damage to or the destruction of any item of property other than the defective product itself.

[75] Tribunale di Milano, 31 gennaio 2003, in Resp. civ. e prev., 2003, 1151 with commentary by S. Della Bella, Cedimenti di scala estensibile e responsabilità del produttore - progettista: la nozione di danneggiato nella disciplina sulla responsabilità del produttore.

[76] Article 9. For the purpose of Article 1, 'damage' means: (a) damage caused by death or by personal injuries;
(b) damage to, or destruction of, any item of property other than the defective product itself, with a lower threshold of 500 ECU, provided that the item of property:
(i) is of a type ordinarily intended for private use or consumption, and
(ii) was used by the injured person mainly for his own private use or consumption.
This Article shall be without prejudice to national provisions relating to non-material damage.

[77] Directive 85/374/EEC (the PLD), article 13: 'This Directive shall not affect any rights which an injured person may have according to the rules of the law of contractual or non-contractual liability or a special liability system existing at the moment when this Directive is notified.'

[78] European Court of Justice, C-285/08 - Moteurs Leroy Somer, 4 June 2009.

systems of contractual or non-contractual liability based on other grounds, such as fault or a warranty in respect of latent defects.'[79]

Summing up, in Italy a consumer can seek (alternatively or cumulatively) two forms of protection provided by product liability law, under both the Consumer's Code and the Civil Code.

Tort liability of the manufacturer

Article 103(d) of the Consumer's Code provides a definition of 'manufacturer' that reflects the definition of 'producer' included in article 3 of the PLD.[80] Similarly, the code reflects the definition of 'defective product' of the EU Directive (article 6).[81]

The manufacturer is obliged to:

a. sell safe goods exclusively;

b. provide the users with detailed information on the prevention and evaluation of any risk connected to the ordinary or reasonably foreseeable use of the goods; and

c. adopt any possible measures to make the users aware of the product's risks and how to prevent them. In addition, the manufacturer is obliged to comply with applicable safety standards and rules for the goods.

Article 114 of the Consumer's Code provides for the manufacturer's tort liability. The manufacturer is liable for the damage caused to any third party by its defective goods. Any agreement or contractual clause that excludes or limits in advance such tort liability is null and void.

Product liability is not limited to the manufacturer of the defective product but is also extended to the product's marketer. If the name of the manufacturer is known to consumers, it shall be liable to the marketer. This means that product liability also attaches to importers of products.

The damaged party must claim for damages within three years of the time he or she became aware (or should have become aware) of the damage, the defect, and the identity of the responsible person. Any late claim is ineffective. In any case, the damaged party's claim for damages is extinguished 10 years after the defective goods were placed on the market.

If more than one person can be deemed liable for the same damage, those persons are jointly and severally liable toward the damaged party. In addition, a person who has paid the damaged party has recourse against the other responsible persons. The liability is shared between all responsible persons on the basis of:

a. the risk attributable to each of them;

b. the seriousness of each person's fault; and

c. the consequences deriving from such fault.

Tort Liability of the supplier

There may be cases in which the manufacturer is not identified. In these instances, in principle, liability for defective products still lies with the manufacturer. However, it will rest, since the manufacturer is not available, on the importer and distributor.

According to article 3.3 of the PLD, 'each supplier of the product shall be treated as its producer unless he informs the injured person, within a reasonable time, of the identity of the producer or of the person who supplied him with the product. The same shall apply, in the case of an imported product, if this product does not indicate the identity of the importer referred to in paragraph 2,

[79] Ibid. C-285/08 - *Moteurs Leroy Somer*, paragraph 23.

[80] Article 103(d) Consumer's Code: 'any manufacturer of goods or supplier of services, or an agent thereof, or any importer of goods or services within the European Union or any natural or legal person presenting himself as the manufacturer by identifying the goods or service with his own name, trademark or other sign having a distinctive character.'

[81] A good can be considered "defective" when it does not provide the safety that one can reasonably expect, taking all circumstances into account, including: (i) the way in which the good is distributed and its packaging, evident features, instructions, and warnings; (ii) the use to which the good can reasonably be placed on the market and the life cycle which the good can be reasonably expected to undergo; and (iii) the period during which the good was distributed. Finally, the good is considered to be defective if it does not offer the safety normally offered by similar goods.

even if the name of the producer is indicated.' Similarly, under article 116 (*Responsabilita' del fornitore*) of the Consumer's Code (Dlgs. 206/05), the damaged party has the right to obtain from the supplier the manufacturer's name and address. If the supplier fails to reply to the request of the damaged party within three months and the manufacturer is not identified in any other way, the supplier is subject to the same liability as the manufacturer. In the case of a trial initially started against the supplier, the manufacturer can be requested to attend the trial at any time as an interested party. If the manufacturer does not challenge such a request and attends the trial, the trial continues exclusively against the manufacturer, and the supplier is considered free from any liability to the damaged party.

Liability for dangerous products

Article 2050 ICC provides that whoever injures another party in carrying out an activity that is dangerous per se is strictly liable for damages unless the person proves that he or she adopted all possible measures in order to avoid the damage.

As Boscarato explains[82], 'article 2050 covers both conducting a dangerous activity as a continuative and repetitive series of events, and the execution of individual dangerous events, which may even be independent of, and uncoordinated with, each other. Article 2050 is mainly used with regard to liability of an entrepreneur in conducting dangerous activities. However, its area of application is not exclusively restricted to an entrepreneur, since the article does not provide for any restrictions. The rationale behind the article remains that of protecting third parties from damage resulting from certain types of activities, no matter whether or not such activities are conducted within the framework of entrepreneurial activity.' For instance manufacturers and distributors (suppliers) of 'dangerous activities' – such toxic chemical products and blood derivatives.

Like the strict product liability regime implemented in the Consumer's Code, Article 2050 ICC provides for a presumption of the defendant's liability, independent of the defendant's fault. In principle, Article 2050 ICC can apply only to products that qualified as 'dangerous', by express provision of law or because they are likely to cause damage to the user even if appropriately handled. In a string of cases[83], however, the European Court of Justice stated that Member States may not apply national strict liability systems that provide consumers with a higher level of protection than the Product Liability Directive.

Implications for ebbits

The product liability regime in Italy reflects the European regime established with Directive 85/374/EEC. Arguably the major point of interest and departure from the European regime is the co-existence between tortious liability (ex. article 2043 ICC) and the no fault liability (ex. Directive 85/374/EEC), and the implications this may have on the compensation of non-material damages. This seems relevant if one brings the mind to the moral damages (to, e.g., reputation, dignity) arising out of the unauthorised disclosure of data.

In a string of cases revolving on the protection of health information, the European Court of Human Rights (*Z. v. Finland* , judgement of 25 February 1997; *I v. Finland,* judgement of 17 July 2008; *Armonas v. Lithuania,* judgement of 25 November 2008), consistently recognised a positive duty, falling on states and also private parties, to protect the right to data protection in an alert and appropriate way, if necessary through the imposition of sufficiently high compensations in case of infringements. 2. In an internet of things context, 'things' will communicate with each other and with individuals. It is not unlikely to conceive of personal data being stored and processed in an RFID chip independently, that is, without human intervention by a data controller. In many cases, it may be difficult to identify the responsible entity. In one of the cases mentioned earlier, the European Court of Human Rights recognised a positive obligation to provide technological and organisational measures that could make it easy for the injured party to claim compensation for an unauthorised access to her personal data (I. v. Finland). The court argued that: 'It is plain that had the hospital

[82] Boscarato, C. Who is responsible for a robot's actions? An initial examination of Italian law within a European perspective. In van den Berg, B. & Klaming L. (2011). *Technologies on the stand. Legal and ethical questions in neuroscience and robotics*, 383-403: 400.

[83] E.g., European Court of Justice Decisions No. C-52/00, *Commission of the European Community v. French Republic*; No. C-154/00, *Commission of the European Community v. The Hellenic Republic (Greece)*; and No. C-183/00, *María Victoria González Sánchez v. Medicina Asturiana, S.A.*

provided a greater control over access to health records by restricting access to health professionals directly involved in the applicant's treatment or by maintaining a log of all persons who had accessed the applicant's medical file, the applicant would have been placed in a less disadvantaged position before the domestic courts' (our underlying). The court clarified that the injured party ought not to bear the burden of proof to claim the moral damages. This clashes with the interpretation of the Italin courts, whereby moral damage falls not under the no-fault or strict liability regime of the Consumer's Code (and the PLD), but under the category of tortious liability, where the applicant bears the burden of proof. In another case, *Amann v. Switzerland* (judgment of 16 February 2000, the Court reiterated that 'the storing of data relating to the "private life" of an individual falls within the application of Article 8 § 1 (..)'. This means that, if a data breach occurs, the 'damage' is in eo ipso, in the fact 'data breach' itself. The 'damage' is implied in the violation of the fundamental right to privacy: it is, in other words, itself a 'wrongful act' or 'danno ingiusto', without no need fot the claimant to prove effective damage.

In ebbits application, more than one person can be deemed liable for the same damage. In these cases, those persons are jointly and severally liable toward the damaged party. According to article 114 of the Consumer's Code, however, liability is shared between all responsible persons on the basis of: a. the risk attributable to each of them; b. the seriousness of each person's fault; and c. the consequences deriving from such fault. For the purpose of ebbits, there are important references to 'risk', 'seriousness of the fault', 'consequences of the fault'. In those ebbits environments that are characterised by continuous and seamless processing of personal data, these are several 'risks to rights' (e.g., to the right to privacy, to the right to data protection, access to justice, non-discrimination, etc…) that are not easily discernible, when a project begins. However, it is possible, at the beginning of an internet of things project, to construct a system for the prevention and or identification of potential risks. The Privacy Impact Assessment framework, tallies well with the requirements of article 114, which seeks to nail down responsibility between different entities using 'risk management' as yardstick.

Another implication for ebbits may stem from article 2050, liability for dangerous activities. One could foresee that in the future, more dangerous activities (involving toxic substances, e.g.) will be performed automatically. (Although until today we have not foreseen any such applications for ebbits in particular.) In such cases, the operator will be liable for damage resulting from the conduction of dangerous activity, even when such activity is performed by means of machines. For example, he will be liable for damage caused by technology failing as a result of him not checking the structure before use, or not going through the proper procedure. Once again, the risk dimension of the Future Internet of Things ought to be factored in in advance.

6. Intellectual Property Rights

Intellectual property relates to the legal rights vested in the products of the intellectual activity in the industrial, scientific, literary and artistic fields. The law aims at safeguarding creators and other producers of such intellectual goods and services by granting them certain time-limited rights to control the use made of those productions.[84]

IPR have a relatively broad scope. The rights relate to "literary, artistic and scientific works; performances of performing artists, phonograms and broadcasts; inventions in all fields of human endeavour; scientific discoveries; industrial designs; trademarks, service marks and commercial names and designations; protection against unfair competition; and all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields."[85]

The ebbits platform will provide the link between the businesses on one side and the internet and real – life data on the other. ebbits will collect the relevant data (such as the identity of the physical items, their location at a given time, or physical qualities) from the physical environment by means of sensors, RFIDs, tags and actuators. Such data is then stored and processed on ebbits services, as to enable the extraction of useful knowledge about the production or distribution processes. Data, information and knowledge are transmitted to various stakeholders, i.e. to production managers in the factories but also to consumers in their homes who can check authenticity of drugs and pharmaceuticals, inquire about the origin and qualities of their food purchases or about manufacturers' instructions for use given product.[86]

Above mentioned functionalities of ebbits implies that the ebbits platform will collect and process various types of data and information, as well as handle and distribute knowledge associated with such data. In its operation ebbits platform will rely on various data mining technologies, algorithms and software. In this chapter we will consider to what extent, when and in what circumstances such data and information, its storage and organisation, knowledge so derived, algorithms and software may be subject to the legal protection by the Intellectual Property (IP) rights. The analysis focuses on what constitutes a subject matter of the IP protection, in particular under patents and copyrights.

The IP issues will mostly be tackled from the perspective of ebbits as a right-holder: We will try to consider what might constitute ebbits IP and explain the framework that protects it in a general manner (section 6.1and 6.2). A more specific analysis relating to the protection of data and knowledge (data and knowledge ownership) will be discussed under section 6.3. The potential ebbits responsibility for IP infringements will be disused shortly under section 6.4. We will conclude with a few comments on the legal aspects of Digital Rights Management (DRM) technology (in section 6.5). This chapter provides the general overview of the IP frameworks relevant for ebbits rather then comprehensive and detailed legal IP strategy.

6.1 Intellectual Property Legal Framework – General Comments

Regulation of IP rights consists of many coexisting and complementing layers. The first layer consists of the national IP laws. National laws define the nature, subject matter and scope of the protection by the IP rights. In most cases, the intellectual property right grants an exclusive right, i.e. a quasi-monopoly right allowing the right-holder to prevent others from exploiting the subject matter of their right (i.e. a book, computer programme, invention). Such monopoly is confined to the borders of the state where the right is granted. This territorial restriction of effect of the property rights is often referred to as the principle of territoriality.

The territorial (national) character of IPR quickly became an impediment to countries' and creators' interests in having their creative output protected also outside their home borders. This desire prompted the conclusion of the number of the international agreements. Under such agreements the

[84] WIPO (World Intellectual Property Organization), 'Intellectual Property Handbook', WIPO Publication No. 489 (E), Second Edition (2004) (further referred to as WIPO Handbook) http://www.wipo.int/about-ip/en/iprm/index.html (retrieved on 03.12.2013).

[85] Article 2 (viii) of The Convention Establishing the World Intellectual Property Organization (WIPO), Stockholm, 1967.

[86] ebbits website, http://www.ebbits-project.eu/articles.php?article_id=2, last accessed 03.12 2013. Concrete use scenarios are described under sections 3.4 and 3.5 of this deliverable.

Contracting States grant, under their national laws and within their national territories, the IP protection also to foreign creators, inventors and authors. International IP agreements provide for the common understanding of rights and impose minimum standard of protection.[87] However the harmonisation effect of international conventions is not complete: in most cases conventions impose only minimal requirements, allowing the States to provide for rules that are more beneficial for authors and inventors. Moreover, certain issues are not dealt with under the conventions and were left for the national laws to regulate.

Finally, the European Union (EU) has adopted a number of legislative acts relating to IP.[88] European law complies with obligations imposed by international law, but at the same time harmonises IPR further and often provides for a higher standard of protection than international conventions. Therefore, this paper focuses on European IP law, and refers to national laws of Member States (in particular United Kingdom, German, and Italian laws) where they substantially add to EU regulations.

6.2 Protection of ebbits Intellectual Property Assets

6.2.1 Protection by Patents

A patent is a legal title that allows the patent holder to prevent any third party from exploitation of his invention, even if it is developed independently. Patent law protects inventions having technical character that are novel, that involve an inventive step and that are susceptible of industrial application. The patent protection lasts for the limited period of time, and requires formal filling with the competent authorities.[89]

Regulatory framework

Patents are regulated mostly on national level. It is a national law that grants the protection by patent, defines its condition and scope. A national patent is valid only within the territory of the state who granted it.

Several international conventions however regulate patents.[90] Those agreements provide for protection, within a given state, of the inventors from the other Contracting States and for the national treatment (i.e. protection under same condition as the state's own nationals), or right of priority. They tend to focus on procedural matters and often facilitate international patent applications.[91] The European Patent Convention (EPC) is of particular importance for the European legal landscape. The Convention provides the possibility of a single patent application through the European Patent Office (EPO), but also regulates certain substantive aspects of patent protection. The single procedure for granting patents does not mean a single title – to the contrary, European patens consist in fact of the bundle of the national titles: European patent needs to be validated in each State for which it has been granted, and has the same effect as a national patent granted in the respective territory.

[87] The most significant of international conventions include: Paris Convention for the Protection of Industrial Property, 1883; The Berne Convention on the protection of literary and artistic works, 1886, (http://www.wipo.int/treaties/en/ip/berne/); the World Trade Organization's Agreement on Trade-Related Aspects of intellectual Property Rights (TRIPS agreement), 1994; WIPO Copyright Treaty (WCT), 1996; (http://www.wipo.int/treaties/en/ip/wct/).

[88] By means of example: Council Regulation (EC) No 40/94 of 20 December 1993 on the Community trade mark; Directive 98/71/EC of the European Parliament and of the Council of 13 October 1998 on the legal protection of designs,; and Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs; the Directive 98/44/EC of the European Parliament and of the Council of 6 July 1998 on the legal protection of biotechnological inventions.

[89] WIPO handbook, p. 40-42.

[90] I.e., the Paris Convention for the Protection of Industrial Property, 1883; the Patent Cooperation Treaty, Washington (PCT), 1970; Strasbourg Agreement Concerning the International Patent Classification, 1971; TRIPs Agreement, cited above; and Patent Law Treaty (PLT), Geneva, 2000; Council of Europe Convention on the Unification of Certain Points of Substantive Law on Patents for Invention of 1963; and the Convention on the Grant of European Patents, 1973 (European Patent Convention-ECP) and revised 2000 European Patent Convention (EPC 2000).

[91] For the overview of the patent conventions we refer to WIPO handbook, and to Seville, C 'EU Intellectual Law and Policy', Elgar European Law (2009).

Recently, the EU adopted a regulation providing for a EU unitary patent (still not yet in force). The substantive provisions of EU unitary patents are same as those under the EPC convention. Therefore the ECP convention and its rules on patentable subject matter will be discussed first, followed by some examples of national law approaches, to finish with a short discussion on the new EU rules on patents.

Patentable subject matter

Among the EPC's substantive rules relating to the protection by European Patent, the EPC defines conditions for patentability of inventions. ECP provides that protection is granted for inventions in all fields of technology provided that they are new, involve an inventive step and are susceptible of industrial application (Art 52 (1) ECP 2000). In principle all technical inventions fulfilling such these conditions are subject to protection, but the EPC explicitly excludes from the patent protection certain subject matters, such as: (a) discoveries, scientific theories and mathematical methods; (b) aesthetic creations;(c) schemes, rules and methods for performing mental acts, playing games or doing business, and programs for computers; (d) presentations of information (Article 52 (2) ECP). Additionally, the ECP states that European patents shall not be granted for inventions where exploitation would give to rise concerns of "ordre public" or morality; for plant or animal varieties or for essentially biological processes for their production; and for therapeutic or diagnostic methods.[92]

From the ebbits perspective, the exclusion of mathematical methods and computer programs are of particular concern. The mathematical algorithms will in principle not be patentable, unless they serve an adequately defined technical purpose for which protection may be permitted.[93] As regards computer programmes, Article 52 (2) of the ECP convention expressly excludes ordinary computer programmes from patentability. The Convention allows, however, for the patentability of so called computer-related inventions. The difference between ordinary computer programs and patentable computer- related inventions is not straight-forward. The distinction seems to lay in the fact that computer- related inventions produce a further technical effect going beyond the ordinary physical interaction between programme (software) and the computer (hardware) which is characteristic for ordinary computer programmes.[94] Some scholars' say that the EPO interpretation is too broad (and will encompass any invention which makes use of, or embodies some form of technology (hardware))[95] which has resulted in a substantial number of patents for computer-related inventions being granted. It cannot be excluded that the ebbits platform or its parts may qualify as the computer-related invention(s) eligible for protection by European patents. However, definite determination in that respect requires very careful and case-specific consideration which goes beyond the scope of this deliverable.

It has to be noted that, as the EPC is a system merely complementary to the national patents, national laws might adopt different approaches as to the conditions for patentability and definition of the patentable subject matters. In particular national laws might adopt more lenient or strict approaches to protecting software by patents.

The UK

In the United Kingdom, patents are regulated by the Patent Act of 1977, which contains analogous provision to article 52(2) of the EPC excluding computer programmes from protection.[96] UK law

[92] Article 53 of EPC stipulates that European patents shall not be granted in respect of:

(a) inventions the commercial exploitation of which would be contrary to "ordre public" or morality; such exploitation shall not be deemed to be so contrary merely because it is prohibited by law or regulation in some or all of the Contracting States;

(b) plant or animal varieties or essentially biological processes for the production of plants or animals; this provision shall not apply to microbiological processes or the products thereof;

(c) methods for treatment of the human or animal body by surgery or therapy and diagnostic methods practiced on the human or animal body; this provision shall not apply to products, in particular substances or compositions, for use in any of these methods.

[93] Guidelines for Examination in the European Patent Office, Part G - Chapter II-3. Section 3.3, http://www.epo.org/law-practice/legal-texts/guidelines.html, last accessed on 4.12.2013.

[94] Guidelines for Examination in the European Patent Office, Part G - Chapter II-5, Section 3.6.

[95] Bently, L. and B.Sherman, J 'Intellectual Property Law', third edition, Oxford (2009), p. 414.

[96] Section I-(2) of the Patents Act 1977 (Chapter 37, as amended up to the Patents Act 1977 (Amendment) Regulations 2011) reads: It is hereby declared that the following (among other things) are not inventions for the purposes of this Act, that is to say, anything which consists of - (a) a discovery, scientific theory or mathematical method; (b) a literary, dramatic, musical or artistic work or any other

does not preclude patents for the computer-related inventions, thought this exception seems to be interpreted more rigorously than by EPO.[97]

Germany

In Germany the patent law follows the EPC wording and also explicitly excludes patentability of ordinary software. Additionally, German law does not allow patenting of the reproduction of data in general and programmes for data processing equipment.[98] Furthermore, invention is patentable only if it has a technical character and is not yet belonging to the existing available technology (‘Technizität’).[99] The BGH decided that computer programmes can be patented under certain circumstances,[100] (and with due regard to the obligation to define the technical problem that is solved by given invention, in this case the computer programme).[101] Hence, the courts will apply rigorous standards in analysing the patentability of software, and focus on the technical aspect of the invention. In any case, the patentability of computer programmes in Germany remains a difficult and controversial issue.[102]

Italy

Computers programs are also in principle excluded from patent protection in **Italy**[103].

EU unitary patent

To date, in the field of patents, there is no EU legislation in a force, but this is to change soon[104]. In December 2012, the EU adopted a set of laws on patents creating the European unitary patent. The regulatory patent ‘package’ consists of regulation creating a European patent with unitary effect (or 'unitary patent'),[105] and a regulation establishing a language regime applicable to the unitary patent.[106] These regulations are complemented by international agreement among Member States setting up a single and specialised Patent Court.[107] The new EU system creates a unitary patent, i.e. providing uniform protection and having equal effect in all the participating EU Member States.[108]

The EU unitary patent is linked with the EPO patent systems: patent applications are addressed and handled by the EPO. In order to obtain unitary effect, patent holders need to request the unitary

aesthetic creation whatsoever; (c) a scheme, rule or method for performing a mental act, playing a game or doing business, or a program for a computer; (d) the presentation of information.

[97] Bently, L., Sherman, B., op. cit., p. 419.

[98] Patentgesetz (zuletzt geändert durch Gesetz vom 31. Juli 2009):
„§1(3) Als Erfindungen im Sinne des Absatzes 1 werden insbesondere nicht angesehen:
1. Entdeckungen sowie wissenschaftliche Theorien und mathematische Methoden;
2. ästhetische Formschöpfungen;
3. Pläne, Regeln und Verfahren für gedankliche Tätigkeiten, für Spiele oder für geschäftliche Tätigkeiten sowie Programme für Datenverarbeitungsanlagen;
4. die Wiedergabe von Informationen.‟

[99] Ibid. §3 (1) ‚‛Eine Erfindung gilt als neu, wenn sie nicht zum Stand der Technik gehört.‟

[100] Bundesgerichtshof. GRUR 2000, Seite 1007 & Bundesgerichtshof. Beschluss vom 17. Oktober 2001 in der Rechtsbeschwerdesache X ZB 16/00 ‟Das Patentierungsverbot für Computerprogramme als solche verbietet, jedwede in computergerechte Anweisungen gekleidete Lehre als patentierbar zu erachten, wenn sie nur - irgendwie - über die Bereitstellung der Mittel hinausgeht, welche die Nutzung als Programm für Datenverarbeitungsanlagen erlauben. Die prägenden Anweisungen der beanspruchten Lehre müssen vielmehr insoweit der Lösung eines konkreten technischen Problems dienen.‵ BUT this is different if the computer programme, sich durch eine Eigenheit auszeichnet, die unter Berücksichtigung der Zielsetzung patentrechtlichen Schutzes eine Patentierbarkeit rechtfertigt‟.

[101] Compare with Bundesgerichtshof. Beschluss vom 19. Oktober 2004 in der Rechtsbeschwerdesache betreffend der Patentanmeldung 10136238.2. & Bundesgerichtshof. Beschluss vom 19. Oktober 2004 in der Rechtsbeschwerdesache betreffend der Patentanmeldung 100 49 825.6

[102] Blind, K., Edler, J., Nack, R., Starus, J’Software-Patente. Eine Empirische Analyse aus Ökonomischer Und Juristischer Perspektive’, Physica-Verlag: Heidelberg (2003).

[103] Codice della proprietà industriale (decreto legislativo 10 febbraio 2005, n. 30, aggiornata con le modifiche introdotte dal decreto-legge 24 gennaio 2012, n. 1, convertito con modificazioni dalla legge 24 marzo 2012, n. 27)

[104] The new EU unitary patent will apply from 1 January 2014 or the date of entry into force of the Agreement on a Unified Patent Court, whichever is the later;

[105] Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection.

[106] Council regulation (EU) No 1260/2012 of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection with regard to the applicable translation arrangements.

[107] Agreement on a Unified Patent Court, 19 February 2013.

[108] While there are 28 Member States of EU, only 25 States participate in new EU unitary patent system: Spain and Italy opted not to participate in the EU patent system; Croatia joined EU after adoption of the patent package but is likely to join the system.

effect at the EPO. The unitary effect which is then entered by the EPO into its Register transforms the European patent into one single patent for the 25 Member States, with no further need for any validation of a title at national level. Also, the EPO continues examining patent applications based on the substantive provisions of European Patent Convention. Hence, the introduction of the EU unitary patent does not change the assessment as to what is and what is not a patentable invention. In particular, the EU unitary patent will not extend the patent protection to ordinary computer programs.

The EU unitary patent does not suppress or replace national patents and national patent laws. Patent applicants should remain free to obtain either a national patent, a European patent taking effect in one or more of the Contracting States to the EPC, or a European patent with unitary effect.

6.2.2 Protection by Copyright

Several important international conventions have been adopted in the fields of copyrights, including the Berne Convention of 1886,[109] and WIPO Copyright Treaty (WCT),[110] signed in 1996.

The EU has enacted a number of directives in the field of copyrights, [111] providing for relatively high level of harmonisation of the substantive copyright within the EU. The Information Society Directive[112] is central to the EU copyright protection system, as it harmonizes in a horizontal manner (in contrary to earlier directives which regulated rights to a specific subject matters of copyright protection sector by sector) more global concepts of copyright like, e.g. the scope of the rights and exceptions.[113]

Copyright covers a variety of works. The European directives do not define the subject matter of the copyright protection, but refers in this respect to the Bern Convention which provides protection for authors in their "literary and artistic works". Such works include any production in the literary, scientific and artistic domain, whatever mode or form of expression,[114] such as, *inter alia*, literary, scientific, musical works, choreography, photographs, cinematographic works or works of architecture, and others. Literary and artistic works are protected as far as they are original (meaning the work needs to 'originate' from the author and cannot merely be the copy of another work[115]) and fixed in some material form[116] (the later includes the server or computer memory). Copyright protects the form of expression of ideas, but does not protect mere facts, data, ideas or principles. It relates to the creativity in the choice and arrangements words, music, shapes, etc.[117]

The ebbits platform will neither create, nor handle and distribute works that are commonly considered as literary and artistic (such as books, music, scientific papers). ebbits focuses on the collection and processing of information from the physical environment relating to production or logistic processes. Again, mere facts and data are not subject to copyright. Also, the data-files or reports merely gathering and presenting data, or other form of expression of such information, may

[109] The Berne Convention on the protection of literary and artistic works, 1886, (http://www.wipo.int/treaties/en/ip/berne/)

[110] WIPO Copyright Treaty (WCT), 1996; http://www.wipo.int/treaties/en/ip/wct/

[111] Directive 2009/24/Ec of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs; Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property; Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and related rights of copyright applicable to satellite broadcasting and cable retransmission; Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights; Directive 06/9/EC of the European Parliament and the Council of 11 March 1996 on the legal protection of databases; Council Directive 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products; Directive 2001/84/EC of the European Parliament and of the Council of 27 September 2001 on the resale right for the benefit of the author of an original work of art,; Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights; Directive 2012/28/EU of the European Parliament and of the Council of 25 October 2012 on certain permitted uses of orphan works.

[112] European Parliament and Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, (further referred to as Information Society Directive).

[113] Tritton, G., Davis, R., Edenborough, M., Graham, J., Malynicz, S., Roughton, A 'Intellectual Property in Europe', London, Sweet & Maxwell (2002), pp. 323-326.

[114] Article 2 of the Berne Convention.

[115] WIPO Handbook, pp. 42.

[116] Article 2(2) of the Berne Convention.

[117] WIPO Handbook, pp. 40-42. Distinguishing the mere facts, data and ideas from their mode of expression may not always be straightforward, especially in case of the software or databases. Software and Databases are discussed below.

lack the creativity and originality to be protected under copyrights. However, the relevance of copyright for ebbits cannot be entirely dismissed: The data and information handled or created by ebbits itself may occasionally be subject to copyright (i.e. the data may constitute copyrightable work e.g. in case of short description of a production plant or a farm, or food information or recipes presented to consumer, if they fulfil condition of originality[118]). Also the descriptions of ebbits platform and services (such as on ebbits webpage or other promotional materials) may be copyrighted.[119] Additionally, copyright may grant protection to software or/and databases operating within ebbits platform (see below).

With respect to works, European copyright law provides several economic exclusive rights.[120] The most relevant in the context of electronic processing and communication (and hence for ebbits) are the right to authorise or prohibit a reproduction (commonly referred to as the reproduction right);[121] and a right to authorise or prohibit any communication to the public, by wire or wireless means (the right relates in principle to broadcasting and online distribution of works, and is commonly referred to as the 'communication to public right').

The rights are subject to number of possible exceptions, and in particular the reproduction right is subject to the so called 'temporary copy' exception, which exempts the user from seeking authorisation for *"a temporary acts of reproduction [...] which are transient or incidental, which are an integral and essential part of a technological process and whose sole purpose is to enable: (a) a transmission in a network between third parties by an intermediary, or (b) a lawful use of work or other subject matter to be made, and which have no independent economic significance."*[122]

The protection by copyright lasts for life-time of the author and 70 years after his death or 70 years from the date of first publication.[123] No formalities are required for copyright protection of works.

Software copyright protection

As mentioned above, in Europe computer programs are, in principle, excluded from patent protection. Software however is protected by copyright as a 'literary work' in the meaning of the Berne Convention. The software copyright protection is regulated by the Computer Program Directive.[124]

The Directive does not define what can be considered to be a "computer program." The recitals clarify that "the term 'computer program' shall include programs in any form, including those which are incorporated into hardware". The copyright protection of software relates to the expression of the computer program. All forms of expression of programs are protected (source code, assembly code and the object code).[125] At the same time, the copyright protection does not extend to the principles and ideas underlying the software, software interfaces[126] or logic, algorithms themselves[127] and programming languages as far as they comprise the ideas and principles.[128]

[118] As described in the Consumer Experience Network scenario in section 3.5.2. above.

[119] It is impossible to identify a priori all potentially copyrightable works within ebbits, hence we provide merely few examples and not the exhaustive list of such works.

[120] Copyright are grants certain moral right to authors, such as the right of paternity (i.e. to be recognised as author), the right of integrity (right to object modification to works if this harms the honour or reputation of an author) and a divulgation right (right to decide whether or not to disclose the rights to public). Moral rights are not harmonised under the EU law, but are granted under national laws and regulated by intentional treaties. Moral rights are granted to authors, and in principle serve purpose other then an economic purpose. Their relevance for ebbits is marginal hence they will not be further discussed.

[121] Article 2 of the Information Society Directive.

[122] Art 5(1) of the Information Society Directive.

[123] Article 1 of the Term Directive. On special provisions regarding cinematographic and audiovisual works see Article 2(2).

[124] Directive 2009/24/Ec of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs, (referred to as Computer Program Directive).

[125] Recital 7 of the Computer Program Directive. Bently, L. in: Dreier, T. and P. Hugenholtz, P (eds.) 'Concise European Copyright Law', The Netherlands (2006), p. 216. The copyright protection also extends to the preparatory design materials which lead leading to the development of a computer program provided that the nature of the preparatory work is such that a computer program can result from it at a later stage" (recital 7).

[126] Article 1 of the Computer Program Directive.

[127]The computer programmers which operate algorithms, e.g. for the purpose of profiling and making recommendations, could as such be protected, Bently, L., In: Dreier, T., Hugenholtz, P. (eds.), op. cit., p. 216.

[128] Moscibroda A., Schnabel Ch., Brison F., Depreeuw S., Gutwirth S., Hornung G., Rossnagel A., Sutterer M., Tertel A., Legal and regulation issues, SPICE Service Platform for Innovative Communication Environment - FP6 Integrated Project, D1.6. (2008), p. 151, available at:

Under the Directive, only the original computer program is protected. The originality criterion requires that the programme must be the author's own intellectual creation,[129] but does not impose the qualitative or aesthetic merits of the program" (recital 8). The author and initial holder of the right is a natural person (group of persons) who has created the program, unless the computer program was created by an employee in the execution of his duties in which case the right are vested with the employer.[130]

The holder of the copyright in a computer programme has the right to control (i) permanent or temporary reproduction of the programme; (ii) its translation, adaptation, arrangement and any other alteration (and the reproduction of those); and (iii) any form of distribution to the public of original or copies of the computer program.[131] Member States are free to extend the protection of the right holder and grant rights that are not foreseen by the directive, e.g. specifically providing a right of communication to the public which would relate to purely electronic distribution of software.

The Computer Program Directive provides for some limitations to the exclusive rights. The exceptions that limit the software copyright protection relate to: [132]

a. acts necessary for the use of the computer program by the lawful acquirer in accordance with its intended purpose, including for error correction;

b. making a back-up copy by a person having the right to use the program, if it is necessary for that use;

c. observe, study or test the functioning of the program in order to determine its underlying ideas and principles by a person having the right to use the program (the reverse engineering exception).

Article 6 of the Computer Program Directive also provides for a decompilation exception. Under that exception, no prior authorisation of the right holder is required where reproduction of code and translation of its form is indispensable to achieve the information necessary to achieve the interoperability of an independently created program. The decompilation right is subject to conditions, such as: (i) the acts related to decomplitaion are performed by the licensee or by any other person having a right to use a copy of the program, or by a person authorised to act on their behalf; (ii) the information necessary to achieve the interoperability has not previously been readily available; (iii) the acts of reproduction or translation are restricted to parts of the original program which are necessary to achieve interoperability; (iv) the information obtained cannot be used to goals other than to achieve interoperability (v) the information obtained cannot be shared with others (unless when necessary to achieve interoperability and (vi) the information obtained cannot be used for development, production or marketing of substantially similar program or any other act infringing copyright.

The Computer Program Directive also obliges Member States to provide for the appropriate remedies against acts of putting into circulation or possession for commercial purposes of infringing copies of the program. Adequate remedies should also be available against acts of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate removal or circumvention of technological protection of the computer program.[133]

Database copyright protection

The ebbits platform will collect and process a range of data from sensors and tags, will store it and organise it in order to make is searchable and useful. Therefore the platform (or parts of the platform) could be seen as database(s).

http://www.ist-spice.org/documents/SPICE_D1.6_FINAL_CC.pdf

[129] Article 1(3) of the Computer Program Directive.

[130] Article 2 of the Computer Program Directive.

[131] Article 4 of the Computer Programme Directive. In the contexts of the Article 4, the right of distribution relates to all forms of the distribution, including the rental, lease, sale, licensing, importation.

[132] Article 5 of the Computer Program Directive.

[133] Article 7 of the Computer Program Directive.

The EU Database Directive[134] provide for the copyright protection of databases. The databases are defined as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means".[135] Databases are protected irrespective of their form (e.g. electronic or print media). Copyright database protection covers the structure of the database (the selection or the arrangement of the data) but does not extend to its content. The database protection also does not extend to the software that is used in the making and the operation of the database.[136]

Databases are protected if they fulfil minimum requirements as to the originality. This condition is expressed in Article 3(1) that grants protection to databases "which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation" (article 3(1)). What the "arranged systematically and methodologically" criterion means (and hence whether the given collection falls under the definition of database under the Directive), and whether the database is original will be determined by the national court in each particular case. However, the mere indexation of items, in an alphabetical (or similar) order, are "sufficiently arranged" to qualify as a "database", but might not fulfil the originality criterion.[137]

The database copyright grants the right-holder the right to carry out or to authorise acts of:[138] (i) temporary or permanent reproduction of database by any means and in any form, in whole or in part; (ii) distribution to the public of a database or its copies; (iii) its communication, display or performance to public, and rental and lending of the databases or its copies.[139]

The Directive also provides certain exceptions to those rights, and in particular the mandatory exception related to the normal use of the database by the lawful user: any of the restricted acts, which are necessary to access the content of the database and for its normal use do not require authorisation.[140] Another exception that might potentially be applicable in case of ebbits platform is exception relating to the use of databases for the purpose of the public security or for purpose of an administrative or judicial procedure.[141]

As in case with other copyright works, no formalities are required for database to be covered by copyright protection.

The Database Directive also provides for a *sui generis* protection of the databases in which a particular substantial investment can be shown. This type of protection is discussed below.

6.3 Data and Knowledge Ownership

Intellectual property law establishes property protection in intangible assets associated with the ideas, knowledge, or information.[142] However, such ideas, knowledge, information (i.e. in form of the raw data, algorithms, know-how) are not as such protected by the traditional IP laws such as copyright, patent law, trade mark or designs. It is the form of expression of an ideas or knowledge that is protected by copyrights, in recognition of creativity in the choice and arrangements of words, music, shapes, etc.

[134] Directive 1996/9/EC of the European Parliament and the Council of 11 March 1996 on the legal protection of databases,(further referred to as a Database Directive).

[135] Article 1 of the Database Directive.

[136] Moscibroda A., Schnabel Ch., Brison F., Depreeuw S., Gutwirth S., Hornung G., Rossnagel A., Sutterer M., Tertel A., 'Legal and regulation issues', SPICE Service Platform for Innovative Communication Environment - FP6 Integrated Project, D1.6., 2008, p155 -157.

137 Hugenholtz, P., in: Dreier, T., Hugenholtz, P., (eds.), op. cit., pp. 316-318. Originality criterion implies the requirement of authorship. Hence, purely computer-made arrangements of data might be refused copyright protection on ground of lack of authorship/originality, thought ultimately the national law determines the issue due to the lack of the precise stipulation on the European level. Moscibroda A., Schnabel Ch., Brison F., Depreeuw S., Gutwirth S., Hornung G., Rossnagel A., Sutterer M., Tertel A., op. cit., p. 155 -157.

[138] Article 5 of the Database Directive.

[139] Article 1 of the Rental Directive.

[140] Certain other exceptions are regulated under Article 6 of the Database Directive, and relate to:
reproduction for private use of the non-electronic database (private copy of electronic database requires the authorisation of the author);use for the illustration for teaching or scientific research; other exceptions to copyrights, traditionally granted under national laws. Those exceptions cannot change the scope of the exception regulated in the Database Directive.

[142] Bently, L., Sherman, B., op. cit., p. 2.

At the same time, a work expressing similar ideas but created independently does not infringe copyright and can be legally exploited by its author. Protection by patents relates not so much to the ideas as such but the technical inventions capable of industrial applications (incorporating such ideas). The IP rights allow to prevent exploitation of protected subject matter (exclusive rights), but their goal is not to restrict access to information or knowledge. The copyright will enable an author to restrict reproduction, performance and communication to public of the protected works. The dissemination of work is thus controlled, however the knowledge and ideas expressed in works can be used freely.

The patents will restrict exploitation of invention (e.g. in form of production and distribution of the patented inventions), however the underlying knowledge and ideas are in fact disclosed and made public in patent application.

It can thus be concluded that the traditional IP law does not provide for the ownership of the data, information and knowledge. Nor does it protect such data, information or knowledge against disclosure: to the contrary, applying for patent protection implies disclosure of the information regarding the invention to the public.

Data, information and knowledge often are important and valuable assets. Below we consider whether there are IP related and other means to protect access and use of such data and information, in particular when it consists of valuable technical or business know-how.

6.3.1 Protection by Copyright

Copyright does not protect facts, data, ideas or principles. The mathematical formulas will thus not be protected by the copyright, neither the business nor the technical idea. The raw data collected and computed by ebbits is not, as such, copyrighted, unless in itself they can constitute the protected work, such as the protected graphical image, protected title, etc. The raw data in the case of ebbits is unlikely to constitute a subject matter of the copyright protection, the potential of restricting access to and exploitation of such data/ information under the copyright is marginal.

ebbits may occasionally collect, create or otherwise use information which might potentially constitute the copyrighted work, e.g. a description of a farm or of a production plant (see also above, sections 3.4 and 3.5), but also e.g. report expressing knowledge derived from raw data and alike. Should ebbits have rights in such works (either because ebbits created it and hence it is an original owner of rights or because ebbits acquired rights under the licence), it may invoke copyright protection. It should however be remembered that copyright protects a form of the expression of the idea rather than the idea itself. Hence, the copyright may prohibit making a copy of the said report (or of its parts) or communicating it to public. The copyright, however, will not protect against expressing same ideas and knowledge in a different form. Consequently, the copyright may contribute to protecting ideas/knowledge by limiting access to and restricting exploitation of works expressing such knowledge/ideas, copyright will not be effective instrument to prevent their divulgation and re-use.

The obligations to a potential ebbits platform from handling third parties' copyrighted material are discussed below.

6.3.2 Sui generis Data Base Rights

As mentioned above, one can examine whether the ebbits platform is a protected database , due to originality in selection and arrangements of its elements, by copyright. As described above, the database copyright protection relates to the structure of the database, and does not protect the aggregated data themselves.

Independently from the copyright protection, the Database Directive provides for so called sui *generis* protection of databases, which is the right that does not fall into copyright or any other category of the intellectual property rights. The *sui generis* right does not aim to reward the creativity of the database maker, but instead aims at protecting his investment in creating a database rather than the creative input of the database maker. Therefore, to benefit from the protection, the maker of the database needs to show a substantial investment in either the obtaining, verification or presentation of the contents of the database. The investment is assessed on the basis of qualitative (e.g. particular skill applied in the process of construction or selection of material for database) or quantitative criteria (investment of time and money).[143] The *sui generis* right is granted to the person who initiates and finances the making of the database,[144] and lasts for a period of 15 years starting from making the database available to the public (with possibility to extend the period of protection in case of substantial changes to the content of the database).[145]

The *sui generis* right prohibits the extraction and/or re-utilization of the whole or of a substantial part of the contents of that database.[146] Extraction or re-utilization of insubstantial parts is not prohibited, unless extraction or reutilisation of insubstantial parts is repeated and systematic *"implying acts that conflict with the normal exploitation of that database or which prejudice the legitimate interest of the maker of the database"* .[147]

Hence, the *sui generis* right relates to the content of the database (in contrast to the copyright database protection relating to the structure of the database). Despite that fact the *sui generis* does not protect the materials/data themselves compiled in the database, or to the facts and data as such[148], it does nevertheless enables the right-holder to restrict the access and use of the database (and its contents).

As in case of copyright, the *sui generis* right is subject to certain exceptions,[149] including the rights to extraction and/or re-utilization of substantial parts of the database for the purposes of public security or an administrative or judicial procedure.

6.3.3 Trade Secrets and Confidential Information

Laws on protection of know-how, trade secrets, confidential business information are often outside the traditional IP legal framework. However, protection of such information is often a valuable ancillary, supplementary or alternative mean of protection of the companies' intangible assets, in particular when the information or inventions in question (or their parts) are excluded from the protection by traditional IP rights (and patents in particular[150]) or when the protection by such traditional rights (in particular by patents) is too expensive[151]. Additionally, companies may opt to protect their assets by secrecy/ confidentiality rather than by IP rights (patent) as they prefer to avoid disclosure of valuable information[152] (while i.e. application for patents protection implies disclosure of the information about invention in question). Also, IP protection is time-limited.

The economic justification to afford the protection to the confidential information lays primarily in (1) providing the additional incentive to innovate by safeguarding the economic/competitive advantage that the trade secret holder can derive from his information, and (2) trade secrets law facilitates disclosure in contract negotiations over the use or sale of know-how that otherwise would not occur in the absence of such protection.[153]

[143] Article 7, Hugenholtz,P. in: Dreier, T., Hugenholtz, P., (eds.), op. cit., p. 329.
[144] Idem.
[145] Article 10 of the Database Directive. Protection starts form the date of the completion of making of the database. The Directive provides 15 years of protection starting from January of the year following the completion of the database, or following the date the database was made available to the public (if such occurs within 15 years before the completion of the database).
[146] Article 7 of the Database Directive. The 'extraction` is defined as "the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form" (Article 7(2)(a)). "Re-utilization" is defined as "any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission" (Article 7(2) (b)).
[147] Article 7(5). See also Article 8 of the Database Directive.
[148] Recital 45 of the Database Directive.
[149] Under Article 9 of the Database Directive. Member States may also allow a lawful user the extraction or re-utilization of a substantial part of the database without the authorisation of the right holder (i) for private purposes of the contents of a non-electronic database (ii) extraction for the purposes of illustration for teaching or scientific research. directive allows Member States to retain the exceptions traditionally granted under the laws similar to the sui generis right (Recital 52 of the Database Directive)
[150] That is when, for example, the information or know-haw do not qualify as patentable subject matter or when the invention represents only incremental invention and hence do not satisfy the 'novelty' test for patent protection.
[151] Baker & McKenzie 'Study on Trade Secrets and Confidential Business Information in the Internal Market' prepared for the European (Commission Contract number: MARKT/2011/128/D) (2013), p. 2, (father referred to as Study on Trade Secrets and Confidential Business Information), available at http://ec.europa.eu/internal_market/iprenforcement/trade_secrets/index_en.htm#maincontentSec2
[152] Study on Trade Secrets and Confidential Business Information, p.13.
[153] Study on Trade Secrets and Confidential Business Information, p. 2.

Currently, the legal protection of business confidential information and trade secrets is almost exclusively regulated by national laws. On the international level a benchmark as to the desirable protection is provided by the TRIPS agreement, nevertheless the TRIPS harmoisation is very limited. The following section presents the TRIPS provision, but then focuses on presenting an overview of various national approaches on what the trade secret is and the means of its protection.

No EU legal act regulates this matter, though the EU Commission has recently proposed the directive relating to the protection of the undisclosed know-how and trade secrets. Given the early stages of the legislative process, it is not possible to predict when the proposal will become the binding law. The main ideas of the proposal are presented below.

The international level

On the international level, the TRIPS agreement provides the base for the protection of the trade secrets by laying down a definition of trade secrets and provides for certain enforcement mechanisms and remedies. Article 39.2 TRIPS stipulate: "Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information:

a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

b) has commercial value because it is secret; and

c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."

However, this provision has not been fully implemented by the sate signatories of TRIPS, or has been implemented with significant differences. Hence it's difficult to speak of a harmonization of trade secrets protection[154] and the legal protection afforded by Member States to trade secrets varies significantly. It appears that only Sweden has a specific legislation regulating trade secrets comprehensively. Other Member States protect trade secrets via different pieces of civil and criminal legislation. Member States' protection of trade secrets is often based on the unfair competition law[155], in other the protection is based on tort law or exclusively on contract[156]. Most of the Member States have general provisions included in labor laws or civil codes to prevent employees disclosing their employer's confidential information and/or trade secrets during the employment relationship.[157]

Trade secrets might relate to very wide range of different information, such as business ideas, algorithms (i.e. a google search algorithm), recipes (i.e. Coca-Cola recipe) the manufacturing process, software the technology and know-how, but also information relating to company's customers or suppliers. Certain condition must be fulfilled for the trade secret to be protected.

There is, however, no unified notion of what is the trade secret or confidential business information. Most Member State adopted similar requirements of protection to those of TRIPS (Article 39 of TRIPS above) and, in order to qualify for the protection, require that the information: (i) is a business related technical or commercial information; (ii) is secret in the sense that it is not generally known or easily accessible; (iii) has economic value consisting of conferring a competitive advantage to its owner; and (iv) is subject to reasonable steps to keep it secret.[158] However the particular elements of such test vary, in particular as regard what is and how to establish the economic value of the information in question.

National laws also vary as to the scope of protection and available remedies. The remedies potentially available to a trade secret owner in case of misappropriation are similar to the remedies applicable to traditional intellectual property rights. Typically, they include injunctive relief and

[154] Study on Trade Secrets and Confidential Business Information, p. 19.

[155] Austria, Germany, Poland and Spain.

[156] Malta.

[157] Except Cyprus, Czech Republic, Republic of Ireland, Luxembourg, Malta and UK, Study on Trade Secrets and Confidential Business Information, p.20-21.

[158] Study on Trade Secrets and Confidential Business Information, p. 5.

damages (such remedies are available in most of Member States); but they may also consist of return, seizure, withdrawal or destruction of infringing goods or materials embedding trade secrets (not available in all jurisdictions). Few member States provide for restraint orders. In any case, such remedies do not seem to be widely used in practice: remedies ordered by courts are often limited to injunctions and damages.

There are also certain risks and problems related to the court enforcement, such a risk of disclosing the secret during the court proceedings (as civil proceedings in many Member States are open to public and grounds for limiting access of the public are limited) or a high burden of proof required for ordering particular remedies.[159] Another factor impairing enforcement of a trade secret – strictly related to the fact that trade secrets are not ranked as IP rights – is the limited possibility of enforcing a trade secret protection against a third party who obtains the information in good faith. In most of the jurisdictions[160] the owner of a trade secret has no action at all against third parties in good faith, unless the third party has acquired or used the secret information negligently. [161]

The United Kingdom

In United Kingdom (as in certain other common law countries such as Ireland) no specific legislation on the trade secrets has been adopted, and their protection is ensured by the common law of confidence and by contracts. Like in Germany, the notion of trade secrets is based on case law rather than on a legislative definition.

Germany

In Germany, the law does not define trade secrets, and the notion is derived from case law and jurisprudence. The protection of trade secrets and confidential information relies on unfair competition law. Unlike in Italy, the action for violation of trade secrets can be brought against anyone who obtained the information, even if in good faith (although damages are unlikely to be awarded in this event)

Italy

Specifically, in Italy the trade secrets are treated as intellectual property, and are protected as such. The specific rules on the protection of the trade secrets have been included into the Italian Code of Industrial Property in Articles 98 and 99. Article 98 affords protection to 'business information and technical-industrial expertise'[162]. Article 99 limits such the owner of such information to stop third party its use only to cases where such third parties obtains and uses such information unlawfully.

The proposal for EU directive

The EU Commission has recently adopted the proposal for the directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (the Proposal). [163]

The Proposal defines the trade secrets in Article 2. Such definition contains three elements: (i) the information must be confidential; (ii) it should have commercial value because of its confidentiality; and (iii) the trade secret holder should have made reasonable efforts to keep it confidential. In this

[159] Study on Trade Secrets and Confidential Business Information, p. 45.

[160] With exception of Austria, Czech Republic, Denmark, Estonia, Finland, Germany, Ireland, Latvia, Lithuania, Portugal and Switzerland).

[161] Study on Trade Secrets and Confidential Business Information, p. 45.

[162] Article 98 reads: "The business information and the technical-industrial expertise, including the subject to the owner's legitimate control, are protected as long as:

a) they are secret, in the sense that they are not, as a whole or in the exact configuration and combination of their components, generally well-known or easily accessible for experts and operators in the field;

b) they have an economic value due to their being secret;

c) they are subjected, by the persons who legitimately control them, to measures which may be deemed reasonably adequate to keep them secret.

2. Data relating to tests or other confidential data the elaboration of which involves a significant effort and the submission of which is a precondition for the authorization to introduce on the market the chemical, pharmaceutical or agricultural products implying the use of new chemical substances, are also protected."

[163] Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, COM (2013) 813 final, 2013/0402 (COD), Brussels, 28.11.2013.

extent the Proposal largely follows definition of the TRIPS Agreement. The Proposal further provides that it is an unlawful acquisition, disclosure and use of trade secrets that will be covered by its provisions. The acquisition, use and disclosure of a trade secret is unlawful in the absence of consent of the trade secret holder and when offender acts intentionally or with gross negligence (Article 3). Article 3 also determines that the use of a trade secret by a third party not directly involved in the original unlawful acquisition, use or disclosure is also unlawful, whenever that third party was aware, should have been aware, or was given notice, of the original unlawful act. In a same time, the proposal explicitly provides that independent discovery and reverse engineering are legitimate means of acquiring information (Article 4).

Next to damages, the remedies that the secret holder may seek in case of his trade secrets misappropriation include: (i) the prohibition of use or disclosure of the trade secret, (ii) the prohibition to make, offer, place on the market or use infringing goods (or import or store infringing goods for those purposes) (iii) and corrective measures. The later relate to, inter alia, the request that the infringer destroy or deliver to the original trade secret holder all the information he or she holds with regard to the unlawfully acquired, used or disclosed trade secret (Article 11).

6.3.4 Protection by Contractual Arrangements

As indicated above, most Member States (except Malta) provide for some form of extra-contractual liability in case of misappropriation of trade secrets, thought its conditions and remedies may vary. Also the recent Commission's legislative proposal will regulate extra contractual liability. Such liability does not preclude, but only supplements the contractual obligations to ensure confidentiality of confidential business information secrets and trade secrets.

The holder of the secrets may enter into contractual arrangements obliging a third party to whom a secret was disclosed to safeguard the secrets. Breach of contractual obligation will result on the contractual liability of infringing party, and may lead to imposition of injunctions or/and damages, It is to be noted that contractual obligations to ensure protection of trade secrets are only enforceable against the parties of such contract.

6.3.5 Conclusions for ebbits

The information that is being collected, created or handled by the ebbits platform, such as information on production processes, industrial recipes, algorithm and mathematical models, technical or business know-how is unlikely to fall under the protection by traditional intellectual property laws. Such information may, however, constitute a valuable asset, and fall under the legal protection of trade secrets. Laws often provide certain remedies in case of misappropriation of trade secrets. The legal protection of trade secrets differs from the intellectual property protection, in particular it does not create monopoly rights and may not be enforceable against a third party who obtain the information constituting the trade secret in a good faith.

Distinction should be made between business confidential information and trade secrets and other confidential information. While the former relate to the business activity, the later may relate to information that should not be disclosed due to the protection of other legitimate interests, including the protection of fundamental rights (e.g. the right to privacy). It needs to be noted that ebbits may be under a legal obligation to protect such other confidential information (i.e. under the data protection framework)

Typically, the information is protected by the trade secret laws only and in as far as its holder keeps it secret. ebbits can and should apply all available measures to preserve the confidentiality and secrecy of the information it handles, including by disclosing the information on need to know basis and subject to by contractual arrangements with third parties aiming to safeguard confidentiality (i.e. confidentiality obligations attached to the license agreements). Also, the technology might be used to restrict and manage the access to confidential information. The later might involve various information managements system and technical protection measures (TPM).

6.4 IP Liability

The ebbits platform may use (i.e. collect, process on its servers, communicate it to third parties) third parties' data, information and knowledge, as well as copyrighted works or inventions protected by IP. Such use may account for acts of exploitation of the subject-matter of IP rights. In such cases, question may arise as to ebbits liability.

In case of patents, ebbits may incur liability when ebbits itself exploits somebody's patented inventions, e.g. by using the third party's patented software (computer-related inventions). ebbits should avoid patent infringement and liability by securing the licence from the patent holder. On the other hand, the mere fact of sharing the information related to third party invention will not subject ebbits to liability under patent law as it does not prevent dissemination of information relating to patented invention.

ebbits may occasionally exploit (i.e. reproduce on and communicate to public) third part's copyrighted works (e.g. few-sentence farm description or alike). Copyright imposes restrictions on exploitation of works, hence a licence should always be sought from the copyright holder to legally copy and to communicate such works to the public.

ebbits may also be under an obligation to protect the trade secrets or confidential information of third parties. ebbits can and should aim to preserve the confidentiality and secrecy of the information it handles by preventing accidental disclosure. ebbits should be able to control who can access given information and ebbits should share such information only on need to know basis and subject to contractual arrangements requiring the protection of confidentiality, and by applying technological measures protecting such information.

6.5 Digital Rights Management

The term Digital Rights Management is used in relation to technological systems that define, manage and protect the rights of access to and use of digital content (e.g. the music or audio file, text and e-books, etc.).[164] DRM allows one to define how and by whom such content may be used, thus implementing the copyright licenses or ensuring the security and confidentiality of data. Such rules are embodied into the content itself (e.g. in a music file, or in case of ebbits in a file with the technical data) and accompany that content to the moment when the digital content is used, reproduced, or exchanged.[165]The rules are expressed in a machine-readable form and automatically enforced hence protecting the content.[166] Technology protection pre-empts infringement and should therefore represents a better level of protection than relying solely upon the law.[167]

Due to their potential to prevent copying and restricting access to the content, DRM is typically associated with the the fight against piracy, and the media industry (music and film industries) has been the major driver behind its development.

DRM essentially refers to three types of technologies: cryptography (modify the original content in order to make it impossible to use it by anyone who is not in possession of the code to decipher it[168]); watermarking (a process which consists in the incorporation of an indelible and invisible digital identification code, i.e., digital watermark, in the content. Such indelible and invisible code contains information relating to and making identifiable the content owner and the terms of the contract[169]),

[164] Caso, R. 'Digital Rights Management,Il Commercio delle informazioni digitali tra contratto e diritto d'autore' CEDAM, Padova (2004). As the author indicates expressions such as 'Rights Management, Copyright Management Systems, Electronic Copyright Management Systems, Copyright Management Schemes, Content Management Systems, Content / Copy Protection for Removable Media indicate similar phenomena.

[165] Mantovani, E., de Hert, P., Habbig, A-K., IPR Issues and DRM Solutions in REACTION Applications, Deliverable of REACTION project (Remote Accessibility to Diabetes Management and Therapy in Operational Healthcare Networks) , FP7 248590, not yet published.

[166] For some, more efficiently then law. For 'software code becomes law' discourse see Lessig, L 'Code 2.0' New York, Basic Books, (2006).

[167] Zittrain, J.L 'Technological Complements to Copyright", New York , Internet Law Series, Foundation Press, (2005), p. 17.

[168] Rosenblatt, B., Trippe, B., & Mooney, S. (2002)., op.cit. p. 91-96. For a critical view on cryptography as janus face technology see Lessig, L 'Code and Other Laws of Cyberspace', New York, Basic Books (1999), p. 35-36.

[169] Rosenblatt, B., Trippe, B., & Mooney 'Digital rights management: business and technology', New York (2002), p. 98.

and fingerprinting (similar to watermarking, but differs from it because, unlike watermarking, the fingerprint is not embedded in the file).[170]

The law recognises the potential of DRM to protect against the copyright infringements but, at the same time, it recognises that such technology might be vulnerable to countermeasures. Hence, copyright law establishes the protection of such technology (the so called "third layer" of protection), by prohibiting the acts of circumvention of technological measures and/or dealing in (commercialisation of) circumvention technology.

A second aspect of DRM is not related to copyright enforcement, but to DRM being used to manage confidential information and to insure data security. In these contexts, DRM systems may ensure protection of trade secrets, but also enable the data processing is in compliance with privacy and on data protection laws.

Finally, the use of DRM may pose some privacy concerns as discussed in Section 6.5.3.

6.5.1 The Protection of DRMs

European law addresses technological measures by means of three directives: the Computer Programme Directive, the Conditional Access Directive[171], and the Information Society Directive.

First, the Information Society Directive defines a technological measure and Rights Management Information (RMI), both being a part of a broader concept of Digital Rights Management (DRM).

Technical Measures are defined as "any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, which are not authorised by the right holders of any copyright, related right or sui generis right in the databases". This is a broad definition which encompasses hardware and software measures, access and use control mechanism, but also measures to protect the integrity and authenticity of the protected content or of device security features.

The legal protection of such measures under the Information Society Directive consists of:

protection of the effective technological measures against any acts of circumvention, which the person concerned carries out, knowing, or with reasonable grounds to know, that he is pursuing that objective; and

prohibition of commercialisation (i.e. manufacturing, importation, distribution, provision for sale or rental, advertisement for sale or rental, or being in possession for commercial purposes) of the material which is presented as suitable to circumvent the protection or which has as its obvious purpose the circumvention.[172]

The Information Society Directive also protects the information about the rights management.[173] The information is protected, if it is associated with a copy of the content or if it appears in connection with its communication to the public.[174] The Directive prohibits:

- Removing or altering the information concerning the rights management systems by any unauthorised person,
- Distribution (of physical copies or otherwise, e.g. by electronic means) of works or other protected subject-matters from which electronic rights-management information has been removed.

[170] Mantovani, E., de Hert, P., Habbig, A-K., op. cit.

[171] Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access, (Conditional Access Directive).

[172] Article 6(2) of the Information Society Directive.

[173] Article 7(2) of the Information Society Directive defines right-management information as *"any information provided by right holders which identify the work or other subject matter, or sui generis rights [...], the author or any other right holder, or information about the terms and condition of use of the works or other subject matter, any numbers or codes that represent such information."*

[174] Thus, watermarking systems are likely to be considered as rights-management information. See Bechtold, S., in: Dreier, T., Hugenholtz, P., (eds.), op. cit., p 397.

Such restrictions apply as far as a person undertaking such acts actually knows that he is inducing, enabling, facilitating or concealing an infringement.[175]

The ebbits platform might occasionally process copyrighted works; however, the ebbits platform is not aiming at the distribution copyright protected media products (such as music, books or audio-visual content as such). Hence, the relevance of DRM (and the legal protection of DRM-related technology) for ebbits in the context of copyright infringements is limited, and most likely reduced to the protection of ebbits software.

However, while the Information Society Directive's provisions in respect of the technical protection measures are the most comprehensive, they are not applicable to software. The software technological protection measures are only regulated sunder the Computer Program Directive, and their protection is limited to prohibition of putting into circulation, or the possession for commercial purposes of any means of which the sole intended purpose is to facilitate removal or circumvention of technological protection of the computer program.[176] The Computer Program Directive does not forbid the act of circumvention itself.

Finally, the Directive Conditional Access Directive prohibits the following activities:[177.]

- the manufacture, import, distribution, sale, rental or possession for commercial purposes of illicit devices[178];
- the installation, maintenance or replacement for commercial purposes of an illicit device and
- the use of commercial communications to promote illicit devices.[179]

The Directive applies when the illicit device is used to enable free access to certain protected services, i.e. TV or radio broadcasts and information society services[180] (defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services"[181]) and to and provision of conditional access as such. [182]

Ultimately, the provisions of on legal protection of DRMs provide the right holder with the additional legal claim to enforce his underlying copyright, i.e. the right holder will be able to bring the claim against the illegal act of circumvention or commercialisation of circumvention technology instead or next to the claim against the unauthorised reproduction or communication to public of a work (software) which was protected by copyright and by circumvented technology.

6.5.2 DRMs as an Instrument to Ensure Confidentiality

Privacy and data protection laws may impose obligations on ebbits to protect security[183] and confidentiality of personal data[184]. Also, the confidentiality clauses in the contracts entered into by ebbits may oblige ebbits to protect the business confidential information and trade sectors of its contact parties. ebbits itself may be interested to technically protect its own trade secrets.

As mentioned earlier, DRM consists of technologies that associate the access and usage rules with the given content. Such rules are following the content (data) and control the way this content

[175] Article 7 (1) Information Society Directive.

[176], Article 7(3) Computer Program Directive.

[177] Article 2(e) of the Conditional Access Directive.

[178] The directive defines the illicit device as *"any equipment or software designed or adapted to give access to a protected service in an intelligible form without the authorization of the service provider".*

[179] Article 4 of the Conditional Access Directive.

[180] Article 2(a) of the Conditional Access Directive.

[181] Article 1(2) of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services .

182 Article 2(a) of the Conditional Access Directive.

[183] Article 17 of Directive 95/46/EC requires states and private parties to 'implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.' 'Having regard to the state of the art and the cost of their implementation, such measures,' continues the Directive, 'shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.'

[184] Personal data can be collected and processed (including their transfer) essentially with the consent of data subject, and in any case should be limited tow what is necessary (data minimisation principle). As regards the requirements of data protection legal frameworks relevant for ebbits please see section the following chapter.

(data) is being used. Hence its potential for automatic enforcement of pre-defines confidentiality requirements.

It is for ebbits to asses to what extent such rules may be associated with raw data that is collected by the ebbits platform from particular physical environments (i.e. the data related to energy consumption in car production plant) to ensure such data is only accessed by authorised parties (i.e. the entity for which ebbits implemented given service, i.e. the responsible members of the particular car factory) and to prevent this data from being access and used by non-authorised entities (competitors, energy suppliers, whether or not they are themselves using ebbits platform). DRM, and in particular watermarking and fingerprinting, could also facilitate monitoring data security breaches and data leaks, as it enables establishing from where given information originates.

6.5.3 Privacy Concerns Associated with DRMs

The application of DRM may raise some concerns as to the privacy protection of individuals. DRM systems might require identification and authentication of users having rights to the content, and hence are able to monitor individual's interest in particular type of the information, e.g. DRMs are able to monitor how many times users access particular content, how long, what other content they like, etc. In ebbits context, DRM and privacy will clash in case the DRM collects and process the information relating to individuals, e.g. when a DRM collects the information about a consumer consulting the particular food information (or alike), which in term indicates his nutritional habits (e.g. person is vegan) or other preferences (when a person looks for halal meet, which may suggest that a person is Muslim).

When application of the DRM technology leads to collecting or processing of personal data, privacy and data protection safeguards apply. Recital 57 of the Copyright Directive states, that any rights-management information systems should incorporate privacy safeguards in accordance with data protection and privacy legislation. In this connection, the EU Article 29 Working Party advised[185] to consider equipping the DRM protection system with privacy enhancing technologies (PETs).

6.6 Intangible Assets

ebbits is likely to produce or use may intangible assets, such as computer programmes, literary or artistic works (like images or literary descriptions), databases, valuable raw data, algorithm, industrial recipes. The Intellectual Property legal framework is thus crucial for ebbits in order to, on one hand, secure its own investment, and on the other, the infringement of Intellectual Property of others.

As regards protection of the ebbits valuable intangible assets, their legal protection can be granted by traditional IP laws, and in particular by patents and by copyright, and/or the legal framework for the protection of business confidential information and trade secrets.

6.6.1 Protection by Patent

The patent will protect the invention that is having the technical character and provided that it is new, involves an inventive step and is susceptible of industrial application.

The patent protection lasts for the limited period of time (20 years under European Patent Convention).

It requires formal filling with competent authorities. Filing implies disclosure of information regarding the invention in question, and may involve significant costs.

Certain subject matter are excluded form patent protection. In Europe (under European Patent convention) the most significant exclusion form patentability in the context of ebbits are those relating to: scientific theories, business methods, and ordinary computer programmes. The

[185] Article 29 Data Protection Working Party, 'Working document on data protection issues related to intellectual property rights' (WP 104), 2005.

patentability of computer-related inventions (and mathematical algorithm with technical purpose) is controversial.

In principle, the patent application should be filled in each jurisdiction where the patent protection is sought (territoriality of patent protection).

International conventions (e.g. European Patent Convention) may facilitate patent application procedure by providing for possibility of single filling with central patent office.

National laws may vary as to conditions for patentability and patentable subject-matters (hence computer programs may be patentable under the law of some Member States).

6.6.2 Protection by Copyright

- Copyright grants exclusive right to control reproduction and communication to the public of literary and artistic works, as far as they are original and fixed in some material form.
- In the context of ebbits, copyright may provide protection in respect of ebbits software, structure of database(s), other literary works (such as ebbits website or promotional material).
- No formalities are required for copyright protection (although the copyright notices are advisable for asserting the ownership of given work).
- Copyright lasts for the limited period of time (in EU, 70 years after the death of the author or form the date of first publication).

6.6.3 Trade Secrets and Confidential Information

Patents and copyright do not provide for ownership in data or knowledge. Hence, neither patents not copyright will protect algorithms and mathematical models as such, know-how, industrial recipes, valuable raw data. Such assets may constitute business confidential information and trade secrets. Given very limited harmonisation of laws on business confidential information and trade secrets on the international level, and awaiting adoption of EU laws in the field, the protection of business confidential information and trade secrets is granted by the national law of each Member State.

The legal protection of trade secrets differs from the intellectual property protection, in particular it does not create the monopoly right and may not be enforceable against a third party who obtains the information constituting the trade secret in a good faith.

6.6.4 IP liability

The ebbits platform may use (i.e. collect, reproduce or otherwise process on its servers, communicate it to third parties) third parties' data, information and knowledge, as well as copyrighted works or inventions protected by IP. In order to avoid liability for infringement, ebbits should secure the licence from the copyright or patent holder.

ebbits may also be under the obligation of protecting the trade secrets or confidential information of third parties. ebbits can and should aim to preserve the confidentiality and secrecy of the information it handles by preventing its accidental disclosure. ebbits should also be able to control who gains access to information. ebbits should be careful in information sharing, e.g., by providing information only on a need-to-know basis, by subjecting it to scrutiny in terms of confidentiality requirements and by applying technological measures protecting such information.

A licensing and contracting process within ebbits may be facilitated by the use of the standard contracts and 'half- automated' contracting (like in case of dialog boxes used for software licencing).

6.6.5 DRM

The term Digital Rights Management is used in relation to technological systems that define, manage and protect the rights of access to and use of digital content (e.g. the music or audio file, text and e-books, etc.). DRM enables one to define how and by whom such content may be used, thus implementing the copyright licenses or ensuring the security and confidentiality of data.

In the context of ebbits, DRM that is used to protect copyrighted material, such as software, enjoy legal protection under Copyright law. DRM might also be used to manage confidential information and to ensure data security. In these contexts, DRM systems may ensure protection of trade secrets, but also enable that data processing complies with privacy and on data protection laws. Finally, the use of DRM may pose some privacy concerns when it leads to the collecting or processing of personal data. In such cases it is advisable ebbits equipping the DRM protection system with privacy enhancing technologies (PETs).

6.7 General Conclusions on IP Protection

Intellectual Property Law grants the right-holder an exclusive right, i.e. a right to authorise or prohibit using a subject-matter of theirs intellectual property. IP law may serve ebbits to protect its own intellectual assets, but also imposes on ebbits an obligation to respect IP of others.

As regards protecting its own intangible assets, ebbits should consider which form of legal protection is most suitable for each of the assets in question. In doing so, ebbits should take into consideration, initially what type of assets are protected under a given legal title, and what acts are restricted. In particular, ebbits should consider whether certain assets are better protected by traditional IP rights (such as patents and copyright) or by legal protection of business confidential information and trade secrets. The latter might be particularly appropriate for protection of ebbits algorithms, mathematical models, know-how, industrial recopies, and valuable raw data which are unlikely to be protected neither by patens nor by copyright.

ebbits should also consider costs associated with the IP protection (in particular in case of patents), required formalities and time limits of granted protection.

An authorisation (licence) should always be sought form the ebbits partners (users) whenever appropriate (i.e. when ebbits may be undertaking acts of exploitation of their IP).

ebbits may also be under obligation to protect the trade secrets or confidential information of the third parties, To this end, ebbits should prevent accidental disclosure of such information, in particular by controlling who can access given information, sharing such information (if needed) on need to know basis and subject to contractual arrangements requiring the protection of confidentiality, and by applying technological measures protecting such information.

In the context of ebbits, DRM may be used both for the protection of copyrighted works (and software in particular), as well as for the protection of business confidential information and trade secrets or other confidential information (e.g. information protected under data protection and privacy laws).

When application of DRM leads to collecting or processing of personal data, it is advisable ebbits equips the DRM protection system with privacy enhancing technologies (PETs).

7. Data Protection

The aim of this section is to offer a view on data protection law as it applies to the Internet of Things and Services. This is done in order to draw lessons for the services proposed by the ebbits project. Similarly to the previous sections, the EU legal framework and the implementation details in three different Member States: United Kingdom, Germany, and Italy are illustrated.

This section is divided into two parts. Part 1 introduces the European legal framework on privacy and data protection. It points at the linchpin of data protection, the 'fair processing principles', and briefly illustrates the rights of data subjects and the obligations of data controllers. In the light of the potential uses of the ebbitts services, the implications of EU data protection law for workplace privacy are concisely sketched. This general overview precedes specific references to recent regulatory developments which address issues more strictly related to the emergence of internet of things and services applications: profiling, data breach notification, and privacy and data protection impact assessment (DPIA).[186]

Part 2 provides a preliminary, non-exhaustive list of the data protection implications that are likely to emerge in ebbits networked service environment.[187] From the onset, the reader must be warned that the way data are processed and the possible data protection implications, or lack thereof, depend on a variety of factors.

Concrete realities are specific. This means that the applicable regulatory grid and instruments must be assessed on case to case basis, particularly when the technological innovations and their interactions have not been fully explored and exposed. In other words, the application of data protection depends, e.g., on whether data is immediately available or requires technical enhancements or otherwise pried out or constructed, the kind of data – sensitive v. non sensitive, intimate v. non intimate personal information, the form of data it offers (audio, video, documenting behaviour, or noting location only), etc. Depending on what happens to the data (the 'fate of data', using the working of Gary T. Marx[188]) and at what stage, different personal data protection safeguards may be required, or none.

7.1 European Legal Framework

Protection of privacy and personal data in the European Union is based on its Treaties, the EU Charter of the Fundamental Rights (CFR) and secondary legislation, namely the Directives (see below). The CFR includes a fundamental right to private and family life (Article 7) and a fundamental right to data protection (article 8).

Article 8 of the EU Charter of Fundamental Rights states:

> 'Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.'

After the entry into force of the Lisbon Treaty in 2009, the CFR became a legally binding instrument and the Treaties now include explicit reference to protection of personal data. Article 16 (ex article 286) of Treaty on the Functioning of the European Union (TFEU) and article 39 of Treaty on the European Union (TEU) both recognise the right to data protection. The Court of Justice of the European Union in Luxembourg (the European Court of Justice, ECJ) ensures uniform application of

[186] Another important issue that can be conceptually separated from data protection is 'ownership of data', which is addressed in section 6.3.

[187] From SENSEI project (IoT-A report) quoted in Van den hoven http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation

[188] Gary T. Marx is professor Emeritus of Sociology at M.I.T. http://web.mit.edu/gtmarx/www/garyhome.html

the EU law. The court has delivered a number of landmark decisions regarding privacy and data protection: e.g. Lindqvist (C-101/01), Promusicae (C-275/06) or Bavarian Lager (T-194/04).

Article 7 of the EU Charter of Fundamental right or CFR protects the right to private and family life

> 'Everyone has the right to respect for his or her private and family life, home and communications'

This provision echoes the first paragraph of the right to private and family life enshrined in article 8 of the 1950 European Convention on Human Rights (ECHR).[189] Article 8 ECHR is highly relevant since, in Europe, the right to privacy has been shaped by the activism and case law of the European Court of Human Rights (ECtHR). Through a broad interpretation of notions such as 'house', 'communications' and 'privacy', article 8 has been interpreted as protecting also personal data.[190]

The aforementioned EU secondary legislation consists of three "basic" instruments:

Data Protection Directive (95/46/EC)[191] , which is the most stringent one,

ePrivacy Directive (2002/58/EC)[192], as amended by Directives: 2006/24/EC and

- 2009/136/EC,[193]
- Data Retention Directive (2006/24/EC).[194]

Specific instruments, such as Council Framework Decision 2008/977/JHA195 deals with data protection with regard to criminal matters, and Regulation 45/2001196 lays down data protection rules for the EU institutions and bodies.

The European Commission recently launched the process of the revision of these instruments. Currently a draft data protection regulation is being discussed by European Parliament and EU Council. The data protection regulation may be endorsed in 2014.[197] Given its legal status, regulation, it will have direct effects in the member states legal systems.

In addition to 'hard' law instruments, the EU legal framework on data protection includes recommendations by the European Commission, the opinions of the article 29 Working Party[198], the EU body tasked with clarifying data protection ambiguities, and advices from other bodies or agencies, such as the European Network and Information Security Agency (ENISA) and the

[189] Council of Europe (1950, amended version 2010). European Convention on Human Rights. Retrieved 28 January from: http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/Convention_ENG.pdf

[190] See cases *Copland v. UK*, judgement of 3 April 2007, §41; *Halford v. UK*, judgment of 25 June 1997, §44; *Niemietz v. Germany*, judgement of 16 December 1992, § 32; *Peck v. UK*, Judgement of 28 January 2003, §85; *Amann v. Switzerland*, judgement of 16 February 2000, § 65-57).

[191] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[192] Directive 2002/58/EC of the European Parliament an d of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications.

[193] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users ' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[194] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[195] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

[196] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

[197] European Commission. 2012. *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 11/4 draft (including explanatory memorandum).

[198] This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. http://ec.europa.eu/justice/policies/privacy/index_en.htm For a critical review see: Yves Poullet and Serge Gutwirth. "The contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of 'reflexive governance'?" *Défis du droit à la protection de la vie privée .Challenges of privacy and data protection law - Challenges of privacy and data protection law*. Ed. Verónica Perez Asinari & Pablo Palazzi. Brussels: Bruylant, 2008. 570-610. Available at: http://works.bepress.com/serge_gutwirth/63

European Data Protection Supervisor (EDPS). Recommendations and opinions can be categorised as soft law instruments, in the sense that they are not binding on member states. However, each member state can decide to create legal obligations based on the foregoing opinions or recommendations. It is important to underline this because recommendations and opinions contain significant innovative guidelines about how to navigate the regulatory challenges wrought by ebbits-like 'internet of things' services and applications. The most important soft law regulatory initiatives with regards to the Internet of things that are taken into consideration in this document are:

- Commission Recommendation on the implementation of privacy and data protection principles in Applications supported by radio-frequency identification, 12 May 2009[199];
- Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, 13 July, 2010, WP 175[200];
- Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, 11 February 2011, WP 180.[201]

Eventually, at the end of February 2013, the European Commission published the results of a public consultation on the Internet of Things and the output from the work of the group of experts on the Internet of Things. The conclusions identify some major challenges and discuss regulatory options (doing nothing, soft law, and binding law) issues with regard to privacy & data protection and information security.[202]

7.2 Principles, Rights and Obligations under EU Data Protection Law

Data protection is a set of safeguards promoting the transparency and accountability of government and private-sector record holders. While privacy laws proscribe any processing of privacy personal data "unless" necessary, the rationale of data protection is the opposite: normal personal data (as opposed to precise categories of sensitive personal data, mentioned below) is free to move, provided that transparency conditions are respected, namely:

1) the processing must be fair and lawful (fair processing principles) (article 6, Directive 95/46/EC). Article 6 has become the linchpin of data protection. It was incorporated in the expression 'data must be processed fairly for specified purposes' present in article 8 of the CFR, the fundamental right to data protection. This principle, usually indicated as principle of "data minimisation" or "purpose binding", mandates that all processing is both adequate for and limited to a specific purpose.[203] The processing must always be "required" to accomplish some – obviously legitimate, purpose (article 7, Directive 95/46/EC). The processing needs to be *fully justified*; thus processing data because it could be 'useful' (even if obtained by consent), would breach such a requirement.[204]
2) "data subjects" enjoy specific rights vis-à-vis their personal data (e.g., the right to access and rectify personal data);
3) special national data protection authorities have to be created and endowed with investigative powers over data processing and the quality of processed data, with effective powers of

[199] Commission of the European Communities, 12 May 2009, C (2009) 3200, http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf
The Communication is complemented by Commission staff working document accompanying the Commission Recommendation on the implementation of privacy and data protection principles in Applications supported by radio frequency identification," Summary of the Impact Assessment, 12 May 2009Commission of the European Communities, 12 May 2009, SEC(2009) 586, available at http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid200i9impact.pdf

[200] http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/
See also the previous Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology, 19 January 2005, WP 105 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

[201] http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/

[202] European Commission, Conclusions of the Internet of Things public consultation, 28 February 2013; http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation

[203] Gutwirth, Serge. 2012. "Short statement about the role of consent in the European data protection directive" The Selected Works of Serge Gutwirth http://works.bepress.com/serge_gutwirth/80

[204] Compare Article 29 Data Protection Working Party. 2007. *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, 00323/07/EN WP 131, 10.

intervention such as that of ordering the blocking, erasure, or destruction of data, and with the power to engage in legal proceedings.

The relevance of the data protection framework for the notion of personal data is obvious. In order to work, data protection requires a definition of personal data, because only data that is personal comes under the purview of (personal) data protection law. The definition of personal data, however, has not been easy to pin down. The most stringent initiative in this area, the aforementioned Data Protection Directive, provides the general definition of personal data: personal data "shall mean any information relating to an identified or identifiable natural person" (Article 2a).

The same directive (in Article 8.1) recognizes that the revelation of some personal data - the so-called sensitive or special personal data revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health status, or details of sex life(") - poses a potential risk of discrimination. The processing of this sensitive personal data is prohibited in all but a limited number of circumstances that should be applied in a restrictive way as much as possible, such as for the purposes of the provision of care or treatment or in the management of health-care.

In addition, data protection rules deal with information requirements (article 10-11, Directive 95/46/EC) data quality, supervision, adoption of reactive and compensatory measures, duties in case of data leaks or data breaches, which are also part of data protection.

Given the scope of some ebbits applications, it is important to point out the importance of privacy protection in the workplace. European data protection yields protection to privacy in the workplace. This seems relevant for ebbits applications which are planning to include personal information with the data set that follows a product during its life cycle, for instance, through the integration of a certificate identifying a technician performing a certain task. This practice already exists in the aircraft sector industry where each minute of work performed by a technician on an aircraft is noted down and recorded. This could also be applied in other sectors, including in the food cycle production to ensure food traceability. These practices should cope with the fact that, in continental Europe, the privacy of workers in the workplace is protected. In the case *Niemietz v. Germany* (judgement of 16 December1992) the European Court of Human Rights made clear that " to interpret the words private life" and "home" as including certain professional or business activities or premises would be consonant with the essential object and purpose of Article 8 (right private and family life), namely to protect the individual against arbitrary interference by the public authorities (...).' In *Copland v UK* (judgement 3 April 2007), the same court clarified that monitoring employees' emails or phone calls is a violation of the right to private life. Moreover, as suggested in *Halford v. UK* (judgment of 25 June 1997), employees may have a reasonable expectation of privacy in the place of work, which entails making explicit the presence of monitoring technologies and the possibility of objecting surveillance. This boils down to two main principles:

- personal data must be processed fairly and lawfully, also in the workplace, and
- workers must be aware that data about them are being stored and processed.

The informed consent of the person/worker concerned must be sought. In addition, given the peculiar asymmetry that characterise the employer-employee relationship, personal data protection must be supported by collective bargaining mechanisms. According to national labour laws and collective agreements (also at the national level) management may be required to seek the consent of not only individual workers but also of their representatives (e.g., trade unions) when introducing technologies that monitor employees and process personal data.[205]

7.3 Data Breach Notification

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service, across Europe.[206] In recent years, data breaches have become

[205] P. De Hert, 'The Use of Labour Law To Regulate Employer Profiling: Making Data Protection Relevant Again', in M. Hildebrandt and S. Gutwirth (eds), *Profiling the European citizen. Cross Disciplinary Perspectives*, Springer, 2008

[206] Article 2(h), Directive 2009/136/EC amending the e-privacy directive 2002/58/EC, referenced above.

commonplace. Cyber-attacks, hacked passwords, compromised credit card information, and data thefts can lead to personal data being disclosed, traded, exchanged. This may have serious consequences on users' rights and deeply affect trust and system reliability. As indicated in the EU led public consultation on the Internet of Things mentioned earlier, data breaches are likely to augment in the future as data collection and computing rapidly increase.[207] However, the internet of things also allows the adoption of data centric solutions such as 'sticky labels', digital rights management (DRM, discussed in paragraph 6.6) and other technical and organisational measures, that could mitigate the risks of data breaches.

EU law (under the e-privacy Directive 2002/58/EC as amended by Directive 2009/136/EC) makes the duty of 'data breach notification' mandatory on companies operating in the electronic communications sector (telecom providers and Internet service providers (ISPs). In the case of a personal data breach, data breaches have to be reported to regulators, who then will decide whether action against a company should be taken, and potentially to individuals as well. The provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority (article 4.3 e-privacy directive 2002/58/EC). In addition, when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay (article 4.3 e-privacy directive 2002/58/EC). As preambular consideration 59 to Directive 2009/136/EC clarifies, the notification of security breaches reflects the general interest of citizens in being informed of security failures which could result in their personal data being lost or otherwise compromised, as well as of available or advisable precautions that they could take in order to minimise the possible economic loss or social harm that could result from such failures.

As the Preamble to Directive 2009/136/EC recognises, however, the interest of users in being notified is clearly not limited to the electronic communications sector, and 'therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at Community level as a matter of priority'.[208]

It is important to mention that, under article 31 and 32 of the proposed EU regulation, a general data breach notification requirement applicable horizontally to all types of data controllers is introduced, and notification of a breach is to be given by a data controller to both its lead DPA (Article 31) and the data subjects concerned (Article 32). Notification to the data subject is not required if the controller had implemented "appropriate technological protection measures" prior to the data breach (Article 32(3)); this, it has been suggested[209], will provide a powerful incentive for companies to improve their data security procedures and technologies.

While at the level of the EU, there is only one sector-specific requirement for telecom providers and Internet service providers (ISPs) to notify regulators and adversely affected individuals of all security breaches (enshrined in article 4 of Directive 2009/136/EC amending the e-privacy directive 2002/58/EC), EU member states may take additional measures, i.e., they could decide to make mandatory the data breach notification duty beyond telecom providers and Internet service providers (ISPs). A closer look at United Kingdom, Germany, and Italy reveals that:

United Kingdom

The United Kingdom's Information Commissioner's Office (ICO) issued a guidance note on notification of data security breaches to the ICO.[210] The ICO advised that it should be notified of serious breaches, although there is no legal obligation.

[207] ENISA, the EU Agency for Network and Information Security, provides a list of the types of IT-related breaches and risks identified during a survey the EU agency conducted in 2011. The operators surveyed reported actual data breaches and also indicated what are the risk situations likely to lead to data breaches. See ENISA (2012). Data breach notifications in the EU. http://www.enisa.europa.eu/act/it/library/deliverables/dbn/at_download/fullReport.

[208] Consideration 59, Directive 2009/136/EC

[209] Kuner, C. (2012) The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *Privacy & Security Law Report*, 11 PVLR 06, 02/06/2012.

[210] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/guidance_on_data_security_breach_management.pdf

Germany

In Germany, an obligation to issue notifications in cases of data breaches entered into force in September 2009. This obligation is included in Section 42a of Germany's amended Federal Data Protection Act (BDSG).211 Controllers are obligated to notify both the DPA and the data subjects. The law is modelled on the security breach notification laws that have been enacted in the United States. Similarly to the United States approach, the obligation is not a general, but it applies à la carte, i.e., to specific sectors, namely:

- Bank and credit card data
- Telecommunications data and data collected online
- Data related to criminal offences
- Other particularly sensitive data

Italy

Further to article 1. 3 of the law ('decreto legislativo') of 28 May 2012, n. 69, the the notification of data breaches ('Adempimenti conseguenti ad una violazione di dati personali') now features under section 32-bis, paragraph 6, of the Italian Data Protection Code. This provision creates a general obligation to notify the Data Protection Authority and to the individuals concerned. It applies to all the providers of publicly available electronic communications, which are the entities providing the public, on public communications networks, with services that consist mainly or exclusively "in the conveyance of signals on electronic communications networks".[212]

7.4 Attempts to Strengthen the Rights of Individual Data Subjects

As mentioned above, on 25 January 2012, the European Commission released a proposal for a General Data Protection Regulation (GDPR)[213], which may come into force in 2014. In general, the proposed regulation attempts to strengthen the rights of individual data subjects. Under Chapter III, 'Rights of the data subjects', eight long articles, including two innovative ones, the 'right to be forgotten' (article 17) and 'right to data portability' (article 18), detail the individual rights of information (article 14), the right to access (article 15 proposed regulation), the right to rectification (article 16), and the right to object to data processing (article 19).

As mentioned earlier, a general data breach notification requirement applicable horizontally to all types of data controllers is also introduced (article 31). Furthermore, building upon Directive 95/46 'automated individual decisions', article 20 expressly introduces a right not to be subject to measures stemming from "profiling" (see below, paragraph 7.4.1). The other relevant innovation is contained in article 33. If turned into law, article 33 would make privacy impact assessment or data protection impact assessment mandatory (see below, paragraph 7.4.2).

7.4.1 Profiling

Profiling means collecting and using pieces of information about individuals to make assumptions about them and their future behaviour.[214] For instance, a person who buys meat regularly will often buy wine. The logic according to which "people who did this and that often also did x" need not be necessarily built in advance. It can either be determined in advance, or it can be generated from data collected earlier and elsewhere. As a matter of fact, 'profiling implies a shift from *searching and measuring* towards *detecting*: while more classical statistical approaches aim at validating or invalidating proposed correlations believed to be pertinent answers to existing questions, with profiling there are no preliminary questions. The correlations as such become the 'pertinent'

[211] http://www.bfdi.bund.de/EN/DataProtectionActs/DataProtectionActs_node.html

[212] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248

[213] European Commission. 2012. *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 11/4 draft (including explanatory memorandum).

[214] According to article 20 'Profiling" is defined as "a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour" (Article 20(1).

information, triggering questions and suppositions.'[215] The detection of correlations without a preliminary template of questions or logic is possible through profiling algorithms, which refer to the mathematical logic used to make assumptions.

The snag is that, in a context of increased data collection and ever-growing computing power (Internet of Things), algorithms are extremely complicated. This complexity challenges the transparency principle that sustains data protection, as mentioned earlier in paragraph 7.2. According to EDRi[216], there are three main problems with profiling:

First, algorithms are not perfect: the rarer the activity they are used for, the higher the risk of mistakes. In simple terms: profiling should never be used in relation to characteristics that are too rare to make them reliable, nor to make significant decisions about individuals.

Second, profiling is almost a synonymous to filtering. As such it can reinforce societal stratification and lead to discrimination against racial, ethnic, religious or other minorities. Profiling can have these effects even if such sensitive information is not directly used. For instance, eating habits can be correlated to ethnic groups. This requires that both the results of profiling and the underlying algorithms must be diligently monitored.

Third, profiling algorithms are often protected as "trade secrets". This can create a situation of opacity about the logic behind the sorting and filtering. This may lead to the risk that unreliable profiling is used without the required checks and balances to counter its defects.

Article 20 of the GDPR or proposed regulation (not yet in force) regulates the use of "profiling". Article 20 draws on Article 15(1) of Directive 95/46, which grants the right to every person not to be subject to a decision which produces legal effects concerning him, and on the 2010 Council of Europe Recommendation on profiling.[217] The implications of profiling for ebbits are pointed out at the end of this section.

7.4.2 Privacy and Data Protection Impact Assessment (PIA or DPIA)

As indicated in the 2013 EU-led public consultation referenced above, the Internet of Things (IoT) raises pointed legal and ethical issues related to close monitoring of employees, medical surveillance, consumer behaviour monitoring, profiling, targeted advertisements, etc... issues of great salience for citizens and society. In addition, in the context of the Internet of things and services, characterised by machine processed data on persons, new technologies, new problems may arise. A new category of risks emerges, the 'unknown unknowns.'[218]

For these reasons, in 2009, the European commission called on industries to take into consideration also the *likelihood* of risks to individual rights and the *magnitude* of the impact of new technological applications. The Commission decided to address RFID technology, as one of the main enabling ICT of the IoT. The ensuing European Commission recommendation of 12 May 2009 delved on the implementation of privacy and data protection principles in Applications supported by Radio Frequency Identification (the RFID Recommendation, mentioned earlier). It established a requirement for the endorsement by the Article 29 Data Protection Working Party of an industry-prepared framework for Personal Data and Privacy impact assessments of RFID Applications.[219]

The following lines illustrate succinctly the output of such a recommendation, i.e., the Privacy Impact Assessment Framework ("the Framework") for RFID application. This framework is relevant not only because it deals with an important enabling technology, RFID, which plays an important

[215] Serge Gutwirth and Mireille Hildebrandt (2010), "Some Caveats on Profiling", in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), Data protection in a profiled world, Dordrecht: Springer Science

[216] Edri 'European Digital Rights' is an international non-profit association which promotes, protects and upholds civil rights in the field of information and communication technology. The excerpts about profiling are drawn from EDRi papers, ISSUE 06.

[217] Council of Europe, Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Nov. 23, 2010)

[218] Gary T. Marx. 2013. Preface to Wright, D., & Hert, P. de. (Eds.) (2012). *Privacy Impact Assessment*. Dordrecht: Springer.

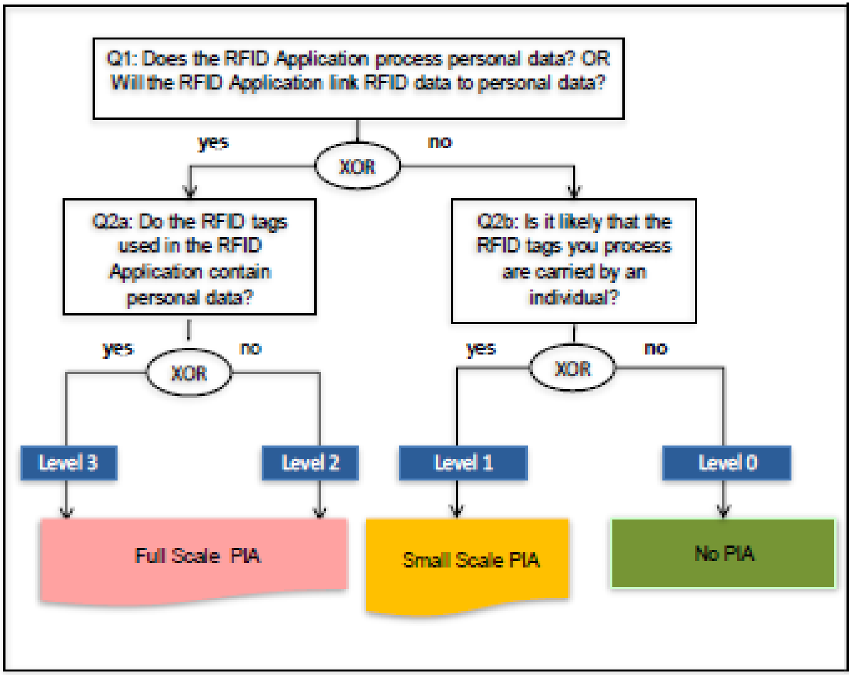
[219] There also exists a DPIA for smart grids. See Article 29 Working Party, *Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force*, 22 April 2013, WP 205. In addition, Privacy and data protection impact assessments, have important precursors in technology impact assessments (TIA) and environmental impact assessments (EIA). As such they can learn valuable lessons from these impact assessment practices

role in ebbits-like services, but also because it is in the context of RFID where the more general idea of conducting Privacy Impact Assessment (PIA) of new technological applications originates. The main source is Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, 11 February 2011, and annexes.

Privacy Impact Assessment can be defined as "a methodology or process for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts".[220]

The PIA process is constructed in two phases.

The first phase is called ***pre-assessment phase***. During this phase, the RFID application is ranked according to a 4 level scale, based on a decision tree (see below). The purpose of this phase is to determine whether a PIA of its RFID Application is required or not. If it is required, the decision tree and the accompanying annexes (described below) help to determine which level of detail it necessitates, i.e., whether a 'Full scale' or 'Small scale' PIA is warranted. This initial analysis must be documented and made available to data protection authorities upon request.


Q1: Does the RFID Application process personal data? OR Will the RFID Application link RFID data to personal data?
yes
XOR
no
Q2a: Do the RFID tags used in the RFID Application contain personal data?
Q2b: Is it likely that the RFID tags you process are carried by an individual?
yes
XOR
no
yes
XOR
no
Level 3
Level 2
Level 1
Level 0
Full Scale PIA
Small Scale PIA
No PIA

Note 1: "Personal Data" as defined by the Directive 95/46/EC (Article 2) 'shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

Note 2: A "RFID Application" is a system that processes data through the use of tags and readers and which is supported by and part of a back-end system and a networked communication infrastructure.

Figure 8 Decision Tree on whether and at what level of detail to conduct a PIA

The second phase is called ***risk assessment phase***. The goal of the *risk assessment phase* is to identify the privacy risks caused by an RFID Application. The risk assessment phase is broken down into four main steps:

- Characterization of the application (data types, data flows, RFID technology, data storage and transfers, etc.);
- Identification of the risks to personal data, by evaluating threats, their likelihood and their impact in terms of privacy and compliance with European legislation;
- Identification and recommendation of controls, in response to previously identified risks;
- Documentation of the results of the PIA, establishment of a resolution regarding the conditions of implementation of the RFID application under review, and information concerning residual risks (PIA Report).

[220] Wright & De Hert. 2012. Op.cit.

Importantly, each step in the risk assessment phase is supported by elements provided in the Annexes of the Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, 11 February 2011. These annexes are important since they provide concrete guidance to companies or party wishing to carry out a PIA.

Annex I is a template describing which characteristics of the (RFID) application must be illustrated. For instance, details about the Application Operator (e.g., Legal entity name and location; Person or office responsible for PIA timeliness; Point(s) of contact and inquiry method to reach the Operator); application overview (e.g., Application name; Purpose(s) of (RFID) Application(s); Basic use case scenarios of the Application; Application components and technology used (i.e. Frequencies, etc.); Geographical scope of the Application; Types of users/individuals impacted by the RFID Application; Individual access and control), etc.

Annex II provides a list of 9 privacy targets that RFID Application ought to respect and take into account, as derived from Directive 95/46/EC. For instance, safeguarding quality of personal data (i.e., Data avoidance and minimisation, purpose specification and limitation, quality of data and transparency as key targets); legitimacy of processing personal data (i.e., legitimacy of processing personal data must be ensured either by basing data processing on consent, contract, legal obligation, etc.); legitimacy of processing sensitive personal data; compliance with the data subject’s right to be informed; compliance with the data subject’s right of access to data, correct and erase data; compliance with the data subject’s right to object; Safeguarding confidentiality and security of processing; etc.

Annex III indicates a set of typical privacy risks, with descriptions and examples. For instance, unspecified and unlimited purpose; collection exceeding purpose; incomplete information or lack of transparency; combination exceeding purpose; missing erasure policies or mechanisms; a lack of transparency of automated individual decisions; uncontrollable data gathering from RFID Tags; etc.

This annex is the core of the PIA. The reason is that privacy risks, once they have been identified, they must be appropriately mitigated through one or more control mechanisms (both technical and organisational). Mitigation measures are outlined in annex IV (below). Control mechanisms should consider the likelihood of risk occurrence and magnitude of impact. (RFID) Application Operators may need to combine controls or augment existing controls based on factors including the technology in use, nature of their implementation, type of information, and applicable policies, among others.

Annex IV gives examples of controls and mitigating measures that can be used in response to previously identified risks. The annex lists five groups of mitigation measures, including: (RFID) application governing practice; individual access and control; system protection measures (including security controls); tag protection; accountability measures. As mentioned earlier, the goal of the risk assessment phase is not only to identify, but also to mitigate the privacy risks triggered by an Application. Once risks have been identified as relevant for an application operator, they can be mitigated through one or several mitigation strategies, some of which are outlined in this Annex IV.

It is recommended that PIA be conducted at an early stage of system development. PIAs are most effective when they are started at an early stage of a project, when: the project is being designed; designers know they want to achieve; they know how they want to achieve their targets; and they who or what is involved.[221]

Additionally, a key element of the PIA is the *Stakeholders consultation*. Article 33.4 of the proposed regulation states that ‘[t]he controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.’ The controller may set up consultation mechanisms by which external stakeholders, whether individuals, organisations or authorities, can interact with them and provide feedback. Data controllers should use consultation mechanisms to gain input from the groups representing the individuals whose privacy will be directly impacted by the proposals, e.g. employees and customers of the RFID operator.’ Stakeholder consultation may be important for

[221] http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/PRIVACY_IMPACT_ASSESSMENT_OVERVIEW.ashx

addressing the data protection issues in some of the projects foreseen by ebbits, where large factories and employees are involved (see below paragraph 7.5 implications).

In the *risk assessment phase,* it is key that companies document how the risks are *pro-actively* mitigated through technical and organisational controls. In this way a PIA plays an important role in compliance with the legal requirements of privacy (Directive 95/46) and it can help assessing the effectiveness of the mitigation procedures. For this reason, the result of a PIA must be formalised in a PIA report, which describes the RFID application and documents the details of the four risk assessment steps referred above. It is important that the report is comprehensive, well drafted and regularly updated. This will enable companies to demonstrate that they have put in place all foreseeable mitigation measures, in case privacy problems occur nonetheless.

Who should do PIAs? PIAs should be performed by organisations, public and private companies, wishing to assess privacy risks and liabilities. In particular, private companies involved in Internet of Things applications are encouraged to adopt PIA process or methodology in their business models. Performing a PIA makes business sense too. It will help private companies avoid expensive, inadequate "bolted- on" solutions, and will contribute towards installing public trust and confidence in a project/product.[222]

Since 2011, the industry-prepared framework for Personal Data and Privacy impact assessment, Personal Data and Privacy Impact Assessment (DPIA), or Privacy Impact Assessment (PIA), has moved from the RFID applications domain, to become what is arguably the most salient innovation of the data protection reform package. If turned into law, article 33 of the proposed regulation would make privacy impact assessment (PIA; the draft regulation uses the term "data protection impact assessment" [DPIA]) mandatory 'where processing operations present specific risks to the rights and freedoms of data subjects [individuals]'.[223]

For the time being, however, in the EU, it is not mandatory to conduct a PIA. As mentioned earlier, the legal basis on which the PIA framework is non-binding recommendation. This means that Privacy impact assessments of RFID Applications can be voluntarily adopted by public and private companies. In principle, member states could, but there is no obligation flowing from the EU law (not yet, at least given the status of the proposed data protection reform), make PIA mandatory in their territories. If made mandatory, member states should require RFID operators to conduct a PIA of applications using, for instance, RFID technology, before they are deployed. Member states would also have to ensure that the RFID operators make the resulting PIA reports available to the competent authority. To date, pending the adoption of the new data protection ratification, the adoption of PIA by private parties is therefore voluntary and depends on the national legal orders.

United Kingdom

In the United Kingdom, there is no statutory requirement for any organisation to complete a PIA. The Information Commissioner's Office (ICO) has produced a PIA handbook to help assess privacy risks and liability. [224]

Germany

In Germany, there is no statutory requirement for any organisation to complete a PIA. The PIA guidelines are based on the EU RFID PIA framework, described below. The German Federal Office for Information Security (BSI) has indicated (symposium, 25 November 2011) that, in the future, the results of privacy impact assessments and the implementation of their results will be important aspects in data protection inspections.[225]

Italy

In Italy, there is no statutory requirement for any organisation to complete a PIA. The PIA guidelines are based on the EU RFID PIA framework.

[222] Wright, D. (2011). Should privacy impact assessments be mandatory?. *Communications of the ACM*, *54*(8), 121-131.

[223] Wright, D. (2013). Making Privacy Impact Assessment More Effective. *The Information Society*, *29*(5), 307-315.

[224] Information Commissioner's Office. 2009. *Privacy impact assessment handbook*, Version 2.0. Cheshire, UK: Wilmslow. http://www.ico.gov.uk/upload/documents/pia handbook html v2/index.html.

[225] German Data Protection authority Website (BSI), https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/RadioFrequencyIdentification/PIA/pia_node.html

7.5 Data Protection Implications for the ebbits Project

In this section, data protection and privacy have been used as synonymous. Privacy as data privacy refers broadly to information self-determination and to the data subject's control and choice over information relating to him or her.[226] The individual should have the possibility to control access to his or her personal information and to construct his or her own public persona. However, this understanding of data protection as informational privacy, as based on fair information principles and individual control, leave untouched important issues that may arise in the context of internet of things. Alternative, more comprehensive assessment tools may be required.

EU data protection law provides a number of important principles, rules, safeguards, recommendations, good practice, etc. that are applicable to ebbits applications. This document highlights four areas of interest to ebbits: workplace privacy, profiling, data breach notification, and privacy and data protection impact assessment (DPIA).

In the area of workplace privacy, data protection law protects the personal data associated (e.g., through RFID tags) with products in their life cycle. In the context of the ebbits project these means that where tags store information about individual workers, such data should be processed fairly and lawfully and not exceed the purpose they were originally collected for. Individual explicit consent of the worker should be obtained, in particular if sensitive data are collected about, e.g., the individual worker affiliation with trade union or health status. Management should also engage workers associations, e.g., trade unions, depending on national labour law, to determine privacy safeguards and limits.

Second, the issue of profiling consumers: Profiling means collecting and using pieces of information about individuals to make assumptions about them and their future behaviour. This is possible through so called profiling algorithms. In the context of ebbits services, consumers must retain the right to object profiling. The right to object should be accompanied by the right to be informed about the techniques and procedures used for profiling, particularly in advertising. Consumers should be informed of the possible consequences of profiling techniques applied to them. Since profiling algorithms are often protected as "trade secrets", this may lead to the risk that unreliable profiling is used without the required checks and balances to counter its defects.

Third, in the context of approach focussed heavily on the 'Internet of Things', the chances of data being lost or leaked is higher. For this reason, it is recommended that ebbits services incorporate in their system architectures data breach notification procedures. It is equally important to keep contact records for customers up to date, ensuring that information is current and accurate. This will avoid missed notifications or notifications being issued to the wrong data subject. Additionally, operators may want to consider the preparation of a list of examples of potential unexpected incidences and seek guidance in advance from authorities in order to avoid any future confusion.

Fourth, and arguably most importantly, Privacy Impact assessment (PIA): Privacy Impact Assessment is a process for assessing the impacts on privacy of a project which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts. In the context of ebbits products and services, it is advisable to carry out an initial analysis seeking to determine whether and to what extent personal data are going to be processed. This should be done in coordination with stakeholders, e.g., trade unions. Should privacy risks or concerns arise, a risk management procedure should identify the appropriate mitigation measures depending on the likelihood and magnitude of the risks and concerns in question.

[226] Westin, Alan F. 1967. *Privacy and Freedom*. New York: Atheneum.

8. Derived Implications to Running the ebbits Platform in a Productive Environment

This section contains the collected implications from Chapters 4, 5, 6, and 7. We found that technology-wise, the ebbits platform does not need significant extensions or changes. However, there are several organizational implications that need to be taken into account when running the ebbits platform productively. The following subsections present them grouped by technical building block.

8.1.1 Implications to the architecture

Implications to the architecture are

- At every technical point where users contribute data (e.g. food receipts, descriptions, ratings) we will make clear under what license the contributed data will be. We propose to use the Creative Commons License as we discussed already in the ebbits deliverable "D1.4 Plan for managing knowledge and intellectual property".
- Privacy concerns arise also from evaluating user interactions. For example, his requests for nutrition details may unveil he is vegan, his preference for halal meat may suggest he is a Muslim etc. User profiles and requests are private by default for that reason in the ebbits middleware and applications.
- The ebbits project should think about protecting its own intellectual properties. As the copyright protection for computer programs does not prevent others from using the same ideas / knowledge, only patents with an additional technical invention would provide sufficient protection.
- As the ebbits project may use or even reproduce databases of other stakeholders and the structure of these databases may be protected under copyright and the content under sui generis data base rights, the ebbits project should make sure that it obtains the necessary permissions from all database owners or should explain that it uses the content for public security which could be the case for the food traceability.
- At the same time, the ebbits project should carefully record its investments into its own database in terms of qualitative (particular skill) and quantitative criteria (time and money) in order to protect the content under sui generis data base rights.

Detecting data breaches play an important role. They consist of the following rules:

- Companies should allocate legal, marketing and technical resources to oversee data breach notification procedures.
- It is important to keep contact records for customers up to date, ensuring that information is current and accurate. This will avoid missed notifications or notifications being issued to the wrong data subject.
- Operators should prepare a list of examples of potential unexpected incidences and seek guidance in advance from authorities in order to avoid any future confusion.

8.1.2 Implications to the knowledge infrastructure

Implications to the knowledge infrastructure are

- The ebbits Trust and Semantic Access Restrictions framework (for details see the corresponding ebbits Innovation Form) will ensure that data is only made available on a need to know basis and respects confidentiality. The access policy is the technical implementation of all present contractual arrangements with the contributor of the data.

- The ebbits project should also apply all available measure to preserve the confidentiality and secrecy of the information it handles, in particular trade secrets, again by restricting access to certain knowledge to certain roles and by attaching confidentiality obligations to license agreements.

8.1.3 Implications to Requirements for the centralised and distributed intelligence

Implications to centralised and distributed intelligence are

- Concerning Digital Rights Management, we do currently not plan to include watermarks, fingerprints or cryptography into the ebbits architecture. Neither for protecting data nor for protecting the ebbits software stack. However we are aware of DRM and will implement it as soon as it is required.
- We see the relevance of DRM not so much to protect our data but to technically state proven correctness and authenticity of data. To ensure for instance that a statement like "this meet has been grown organically" is correct and stems from the farm. However, certified data is no research focus of ebbits. Applications may implement/use DRM at their own choice.

Implications in the Privacy Impact assessment area (PIA) are an important part of the centralised and distributed intelligence. But the impact that IoT applications will have on privacy and other fundamental values cannot be illustrated and pinned down easily at the beginning of commercialization. For this reason:

- It is important to create a team within an organisation to oversee and conduct the PIA. People, groups and organisations that might have a stake in the project, or be affected by it, should be listed and contacted.
- In-depth internal assessment of privacy risks and liabilities. In order to analyse privacy risks, it is quintessential that stakeholders are consulted widely, e.g., trade unions, on privacy concerns and brings forward solutions to accept, mitigate or avoid them.
- The effectiveness of the actions taken to mitigate impact on privacy should not be done once and for all. Reviews concerning new aspects of the projects and new assessments should be factored in.

For the area of profiling data, Chapter 7 provides the following conclusions:

- Consumers have a right to object profiling.
- The right to object should be accompanied by the right to be informed about the techniques and procedures used for profiling, particularly in advertising.
- Consumers should be informed of the possible consequences of profiling techniques applied to them.

8.1.4 Implications to event management and service orchestration

Implications to event management and service orchestration are

- ebbits will use patented technology only if we have a license to do it. To our current knowledge, ebbits does currently not use any patented technology.
- Following the need-to-know basis ebbits will process data only when it is required. It will not process data just because it could be "useful" as elaborated in Section 7.2 on Principles, rights and obligations under EU data protection law.

8.1.5 Implications to physical world sensors and networks

Implications to physical world sensors and networks are

- To ensure confidentiality of data (e.g. measured sensor values for energy consumption) so that it does not get into the hands of competitors we do not plan to use DRM. We rely on a secure network connection and control access with our ebbits trust and access restrictions framework.

In the physical world especially the use of RFID tags requires special rules and strategies. That becomes more important when personal information is tracked and included in processes, too.

- Deactivation of tags in case they store personal information of workers. Any deactivation or removal method should be made available free of charge, either immediately or at a later stage, without any reduction or termination of the legal obligations of the retailer or manufacturer towards the consumer.
- It is important to involve workers and their associations to discuss the potential privacy implications of, say, RFID tags.

8.1.6 General Considerations for productization of the ebbits platform

With regards to product liability but also in general an organization / company developing and owning an ebbits like solution has to establish an end-to-end view from idea generation to development and market success which follows lean governance principles.

The focus on simplicity, flexibility and adaptability that leads to processes that are tailored to business needs, with a relevant set of mandatory process deliverables should use a federated collaboration model with dedicated roles such as:

- Business owner responsible and define overall objectives and are responsible for process implementation and results.
- Process Managers with Network Representatives from the units are responsible for process definition & governance.

With these roles and corresponding tasks and responsibilities the organization / company ensures a standardized development process that minimizes the risk of a product liability issue before the solution is going productive.

Setting the organizational basis is also a pre-requisite for an ISO 9001:2008 certificated software development, maintenance and support process. The results and advices of such a certification give clear insights into the functional correctness of the solution as well as a clear description how to use it as a customer because of the fact that the documentation for installing and using the software is also an integral part of the certification.

During the development certain qualitiy should be to instantiated for several sequences of the overall development process to control and adjust relevant milestone goals.

ICT companies should typically follow the below listed quality gates:

Planning to portfolio Q-gate checking:

- Evaluation process with early adopters
- Prototype development leads to concrete portfolio planning
- Finally portfolio is defined and agreed by involved development units

Portfolio to development Q-gate checking

- Software architecture creation
- Software architecture documentation

Development to production Q-gate checking:

- Product documentation availability (multilingualism ability)
- Software testing
- Product assembly
    - 3rd party product integration

Production to Release Q-gate checking:

- Solution packaging
- Product/solution validation
- Product/solution delivery process

Product liability is defined as the responsibility of a (software) manufacturer to pay damages for injuries or other losses due to a defective product. Since claims might still be made after a number of years, (software) manufacturers are placed in the position of being required retain data to prove that there were no errors during production.

In addition to the above mentioned guidelines and processes the usage of an Information Lifecycle Management (ILM) System should be also mandatory for an organization / company developing and selling an ebbits comparable platform. This allows the transfer and store of data from old systems and then decommissioning of legacy systems (development environments) used before. Nonetheless the data can still be accessed if a product liability issue arises.

With regards to appropriate software usage and customers safety a clear and concise documentation of the installation and usage – also including non-permitted software usage acts – is key for the minimization of product liability issues.

9. Conclusion

This ebbits Deliverable identified, discussed, and evaluated in the context of the ebbits project different kinds of legal, IPR and liability issues. Since none of the project partners has expertise or resources to come up with that result alone, we subcontracted the Vrije Universiteit Brussels to provide the main content of this deliverable.

To bring the discussed legal, IPR, and liability issues into context, we start with Chapters 2 and 3 providing an overview of the ebbits eco-system including typical applications and the resulting legal questions that the consortium came up with.

Chapter 4 provides an overview on Chapters 5, 6 and 7. All four chapters have been provided by our subcontractor Vrije Universiteit Brussels. They discuss Product Liability, Intellectual Property Rights, and Data Protection.

The important question to the ebbits project partners are what implications we draw from this deliverable. We discuss that in Chapter 8. We found that technology-wise, the ebbits platform does not need significant extensions or changes. However, there are several organizational implications that need to be taken into account when running the ebbits platform productively.

The results of this deliverable will help the consortium to advance the ebbits platform in the last project year so that it can be used as the basis of a productive system.

10. References

10.1 References Chapters 1-4

International Energy Agency (1990): IEA Statistics, World Energy Statistics and Balances, 1985-1988 (Organization for Economic Cooperation and Development, Paris)

Sullivan, J.L.m Burnham, A, Wangm M., 'Energy-Consumption and Carbon-Emission Analysis of Vehicle and Component', Center for Transportation Research, Energy Systems Division, Argonne National Laboratory, ANL/ESD/10-6 (2010).

Taillard, D. (2011). Discussion Paper on Voluntary Product Traceability Schemes, Informal expert group on product traceability, Directorate General for Health and Consumers. http://ec.europa.eu/consumers/safety/projects/docs/inventory_discussion_paper_13092011_en.pdf, September 2011

10.2 References Chapter 5

Literature

Atiyah, P, 'The Sale of Goods. (9th ed, 1995)

Boscarato, C. Who is responsible for a robot's actions? An initial examination of Italian law within a European perspective. In van den Berg, B. & Klaming L. (2011). *Technologies on the stand. Legal and ethical questions in neuroscience and robotics*, 383-403: 400.

Bussani , M & Valentin-Palmer, V, *The liability regimes of Europe—their facades and interiors, in* PURE ECONOMIC LOSS IN EUROPE, *supra* note 6, at 120, 148

Clarke, A 'Product Liability' (Sweet and Maxwell. 1989)

Howells, G, Product Liability - A History of Harmonisation, in Towards a European Civil Code (A Hartkamp & E Hondius eds., 2004)

Koziol, H 'Recovery for Economic Losses in The European Union', (2006), Arizona Law Review, 48, 871-895

Lombardi, M and Novellini, G (2012). Product Liability Law In Italy, Mondaq Business Briefing - Jones Day, http://vlex.it/vid/product-liability-law-in-italy-408895054.

Lilienthal., J, (1887), 'Privity of Contract', Harvard Law Review, 1, 5, Dec 15, 1887

Fairgreave, D & Howells, G (2007) 'Rethinking Product Liability: A Missing Element of the European Commission's Third Review of the European Product Liability Direcitve', The Modern Law Review, 70, 962-978

Stanberry., B, (2006) "Legal and ethical aspects of telemedicine", Journal of Telemedicine and Telecare

Stapelton, J (1999) 'Product Liability in the United Kingdom: The Myths of Reform', , *Texas International Law Journal*, 34, 45-70

Stuart., C, (1981), 'Consumer Protection in Markets with Informationally Weak Buyers', 12, 2, 562 – 573

Spindler & Rieckers, Tort Law in Germany § London (Kluwer Internaitonal. 2011). P 39

Reports

Comparative Analaysis of National Liability Systems for Remedying Damage Caused by Defective Consumer Services - A Sudy Commisioned by the European Commision 2004 P106

European Commission 'Third report on the application of Council Directive on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products' COM(2006) 496 Final

Information Society, Commission Factsheet 20, September 2004.

Legal Sources

C-154/00, Commission of the European Community v. The Hellenic Republic (Greece), European Court of Justice,

C-183/00, María Victoria González Sánchez v. Medicina Asturiana, S.A., European Court of Justice,

C-285/08 - Moteurs Leroy Somer, 4 June 2009., European Court of Justice,

C-52/00, Commission of the European Community v. French Republic;, European Court of Justice,

Council Directive 85/374/EEC on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products. OJ L210/29

Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

Donoghue v Stevenson [1932] UKHL 100

Erman-*H. P. Westermann*, § 328 no. 11 ss; Palandt-*H. Heinrichs*, § 328 no. 13 ss.

Italian Consumer's Code - Legislative Decree No. 206/2005

Schuldrechtsmodernisierungsgesetz, 26. Nov 2001 (BGBl. 2001 I 3138).

Supply of Goods and Services Act 1982

Tribunale di Milano, 31 gennaio 2003, in Resp. civ. e prev., 2003

10.3 References Chapter 6

Literature

Article 29 Data Protection Working Party 'Working document on data protection issues related to intellectual property rights (WP 104)', (2005)

Baker & McKenzie 'Study on Trade Secrets and Confidential Business Information in the Internal Market' prepared for the European (Commission Contract number: MARKT/2011/128/D), (2013) http://ec.europa.eu/internal_market/iprenforcement/trade_secrets/index_en.htm#maincontentSec2

Bently, L. and B.Sherman, J 'Intellectual Property Law', third edition, Oxford (2009)

Blind, K., Edler, J., Nack, R., Starus, J'Software-Patente. Eine Empirische Analyse aus Ökonomischer Und Juristischer Perspektive', Physica-Verlag: Heidelberg (2003)

Caso, R (2004) Digital Rights Management,Il Commercio delle informazioni digitali tra contratto e diritto d'autore. CEDAM, Padova.

Dreier, T. and P. Hugenholtz, P (eds.) 'Concise European Copyright Law', The Netherlands (2006)

EPO (European Patent Office) 'Guidelines for Examination in the European Patent Office' (2013) http://www.epo.org/law-practice/legal-texts/guidelines.html

Lessig, L 'Code and Other Laws of Cyberspace', New York, Basic Books (1999)

Lessig, L 'Code 2.0' New York, Basic Books, (2006)

Mantovani, E., de Hert, P., Habbig, A-K 'IPR Issues and DRM Solutions in REACTION Applications, Deliverable of REACTION project (Remote Accessibility to Diabetes Management and Therapy in Operational Healthcare Networks) , FP7 248590, not yet published.

Moscibroda A., Schnabel Ch., Brison F., Depreeuw S., Gutwirth S., Hornung G., Rossnagel A., Sutterer M., Tertel A., 'Legal and regulation issues', SPICE Service Platform for Innovative Communication Environment - FP6 Integrated Project, D1.6. (2008)

Rosenblatt, B., Trippe, B., & Mooney 'Digital rights management: business and technology', New York (2002)

Seville, C 'EU Intellectual Law and Policy', Elgar European Law (2009).

Tritton, G., Davis, R., Edenborough, M., Graham, J., Malynicz, S., Roughton, A 'Intellectual Property in Europe', London, Sweet & Maxwell (2002)

WIPO (World Intellectual Property Organization), 'Intellectual Property Handbook', WIPO Publication No. 489 (E), Second Edition (2004) http://www.wipo.int/about-ip/en/iprm/index.html

Zittrain, J.L 'Technological Complements to Copyright", New York , Internet Law Series, Foundation Press, (2005)

International law

Agreement on a Unified Patent Court, 19 February 2013.

Convention on the Grant of European Patents, 1973 (European Patent Convention 'ECP')

European Patent Convention, 2000 (EPC 2000).

The Agreement on Trade-Related Aspects of intellectual Property Rights, 1994, (TRIPS agreement).

The Berne Convention on the protection of literary and artistic works, 1886.

EU law and EU legislative proposals

Council regulation (EU) No 1260/2012 of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection with regard to the applicable translation arrangements.

Directive 06/9/EC of the European Parliament and the Council of 11 March 1996 on the legal protection of databases (Database Directive).

Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (Term Directive).

Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs (Computer Programmes Directive).

Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services.

Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access (Conditional Access Directive).

European Parliament and Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (Information Society Directive).

Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, COM (2013) 813 final, 2013/0402 (COD), Brussels, 28 November 2013.

Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection.

National law and cases

UK

UK Patents Act 1977

Germany

Patentgesetz (zuletzt geändert durch Gesetz vom 31. Juli 2009)

Bundesgerichtshof. GRUR 2000, Seite 1007 & Bundesgerichtshof. Beschluss vom 17. Oktober 2001 in der Rechtsbeschwerdesache X ZB 16/00

Bundesgerichtshof. Beschluss vom 19. Oktober 2004 in der Rechtsbeschwerdesache betreffend der Patentanmeldung 10136238.2. & Bundesgerichtshof. Beschluss vom 19. Oktober 2004 in der Rechtsbeschwerdesache betreffend der Patentanmeldung 100 49 825.6

Italy

Codice della proprietà industriale (decreto legislativo 10 febbraio 2005, n. 30, aggiornata con le modifiche introdotte dal decreto-legge 24 gennaio 2012, n. 1, convertito con modificazioni dalla legge 24 marzo 2012, n. 27)

10.4 References Chapter 7

Literature

Article 29 Data Protection Working Party, Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, 13 July 2010, WP 175

Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology, 19 January 2005, WP 105
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

Article 29 Data Protection Working Party. Working Document on the processing of personal data relating to health in electronic health records (EHR), 2007, WP 131, 10.

Article 29 Working Party, Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (‘DPIA Template’) prepared by Expert Group 2 of the Commission’s Smart Grid Task Force, 22 April 2013, WP 205

Article 29 Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, 11 February 2011, WP 180
http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/

De Hert, P., (2008). ‘The Use of Labour Law To Regulate Employer Profiling: Making Data Protection Relevant Again’, in M. Hildebrandt and S. Gutwirth (eds), Profiling the European citizen. Cross Disciplinary Perspectives, Springer, 2008

ENISA (2012). Data breach notifications in the EU.
http://www.enisa.europa.eu/act/it/library/deliverables/dbn/at_download/fullReport

European Commission, Commission Recommendation on the implementation of privacy and data protection principles in Applications supported by radio-frequency identification, 12 May 2009, C (2009) 3200
http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

European Commission, Staff working document accompanying the Commission Recommendation on the implementation of privacy and data protection principles in Applications supported by radio frequency identification," Summary of the Impact Assessment, 12 May 2009Commission of the European Communities, 12 May 2009, SEC(2009) 586
http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid200i9impact.pdf

European Commission, Conclusions of the Internet of Things public consultation, 28 February 2013; http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation

European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft (including explanatory memorandum).

Gary T. Marx. 2013. Preface to Wright, D., & Hert, P. de. (Eds.) (2012). Privacy Impact Assessment. Dordrecht: Springer

German Data Protection authority Website (BSI), https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/RadioFrequencyIdentification/PIA/pia_node.html

Gutwirth, Serge and Mireille Hildebrandt (2010), "Some Caveats on Profiling", in Serge Gutwirth, Yves

Gutwirth, Serge. 2012. "Short statement about the role of consent in the European data protection directive" The Selected Works of Serge Gutwirth http://works.bepress.com/serge_gutwirth/80

http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/

Information Commissioner's Office. 2009. Privacy impact assessment handbook, Version 2.0. Cheshire, UK: Wilmslow. http://www.ico.gov.uk/upload/documents/pia handbook html v2/index.html.

Kuner, C. (2012) The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. Privacy & Security Law Report, 11 PVLR 06, 02/06/2012.

Poullet, Y. and Serge Gutwirth. "The contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of 'reflexive governance'?" Défis du droit à la protection de la vie privée. Challenges of privacy and data protection law - Challenges of privacy and data protection law. Ed. Verónica Perez Asinari & Pablo Palazzi. Brussels: Bruylant, 2008. 570-610. Available at: http://works.bepress.com/serge_gutwirth/63

Westin, Alan F. 1967. Privacy and Freedom. New York: Atheneum.

Wright, D. (2013). Making Privacy Impact Assessment More Effective. The Information Society, 29(5), 307-315.

Wright, D. (2011). Should privacy impact assessments be mandatory?. Communications of the ACM, 54(8), 121-131.

Wright, D., & Hert, P. de. (Eds.) (2012). Privacy Impact Assessment. Dordrecht: Springer

Legal acts

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Council of Europe (1950). European Convention on Human Rights. http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/Convention_ENG.pdf

Council of Europe, Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Nov. 23, 2010)

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users ' rights relating to electronic communications networks and services

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the services or of public communications networks and amending Directive 2002/58/EC.

Case law of the European Court of Human Rights

Copland v. UK, judgement of 3 April 2007

Halford v. UK, judgment of 25 June 1997

Niemietz v. Germany, judgement of 16 December 1992

Peck v. UK, Judgement of 28 January 2003

Amann v. Switzerland, judgement of 16 February 2000

11. Table of figures