GO-DIP – MANAGING DIGITAL INTELLECTUAL PROPERTY
IN MANUFACTURING SMES DIGITALIZATION PROCESSES

GO-DIP

Design Option Paper

Grant Agreement Number 970904
Start date of the Project: March 1st 2021
Duration: 12 months

SUMMARY

EXECUTIVE SUMMARY

Industry 4.0 is a process that is leading to fully automated and interconnected industrial production. New Technologies are integrated to improve working conditions and increase the productivity and production quality of plants.
In the context of Industry 4.0, digital technologies enable business to:

- gain competitive advantage;
- expand their markets;
- improve their services.

Digitalisation process in manufacturing SME requires specific skills and competences to implement new technologies within the companies. For instance, it is required to make smart traditional products by creating machine to machine or man to machine interactions.
Such interactions usually allow the collection of data related to the products, for instance: operating parameters, information on the use of the products made by the consumers, etc. All this data needs to be stored, listed, and analysed.
Therefore, to implement digitalisation process manufacturing, SME should support significant investments, starting specific projects to adapt the shape of products or to acquire new technological solutions, software, databases, and a place to store data.

All these intangible assets can be protected by intellectual property rights, depending on the value to be protected. Therefore, to gain competitive advantages and to make the most investment, companies should pay attention to these important legal aspects of the digital transformation process.
Moreover, according to the open innovation business model, often such assets are provided to companies by external providers. In this way, companies somehow became dependent on providers and this could affect the possibility to ensure the continuity of their business.
Therefore, by signing agreements with providers, manufacturing SME should pay attention to some legal aspects that could avoid a complete dependence on providers, in particular with regard to the intellectual property related to digital transformation.
Actually, it is crucial for the companies to ensure themselves the ownership of such intellectual property rights or, at least, the authorisation to access the intangible asset and exploit them without limit.
With the help of this Design Option Paper (DOP), understanding the key concepts of digital data management of small and medium size companies, assisted by intermediary advisory services will result in their being better equipped to incorporate the software and data IP management systems into their business strategies, and thus boost digital innovation in a new dimension.

GLOSSARY

COPYRIGHT	The exclusive, legally secured right to reproduce, distribute, and perform a literary, musical, dramatic, or artistic work. Now the term is commonly subsumed under the broader category of legal regulations known as **intellectual-property law.** Copyright is designed primarily to protect an artist, a publisher, or another owner against specific unauthorised uses of his/her work (e.g., reproducing the work in any material form, publishing it, performing it in public, filming it, broadcasting it, or making an adaptation of it). A copyright supplies the holder with a limited monopoly over the created material that assures him of both control over its use and a reproduction.
DIGITAL INTELLECTUAL PROPERTY (DIP)	The digital IP is the intellectual property in a digital format generated consciously or not by the vast majority of companies.
DATA	Data is an elementary piece of information.
DIGITAL DATA	Information in a digital format that can be shared (transmitted) or used (processed).
DIGITAL DATA DRIVEN INNOVATION	New business models that are interlinked with the exploitation of data and their role in supporting decision-making in the organisations.
DIGITAL DATA PROTCTION	Data protection is the process of safeguarding important information in any digitised form from corruption, compromise, or loss.
DIGITAL DATA PRIVACY	Relates to information privacy, communication privacy and individual privacy. Individual data can be seen as having two types of value: a commercial value and a private value. The fact that data is collected can have both positive and negative effects, and can cause a violation of privacy and a monetary cost.
DIGITAL ECONOMY	Is an economic sector involving all productive, servicing, organisational processes that are based on digital technologies.
DIGITAL RIGHTS MANAGEMENT (DRM)	Protection of copyrighted works by various means to control or prevent digital copies from being shared over computer networks or telecommunications.
OPEN DATA	Data freely accessible to everybody for reuse editing or elaboration without restriction due to copyright and other parties' rights.
FOSS	Free and Open Source Software
SAAS	Software as a service
IAAS	Infrastructure as a service
STAAS	Storage as a service
INBOUND LICENCES	Are groups of rights (in the code) one obtains from upstreaming data from suppliers or when one downloads data.
OUTBOUND LICENCES	Are the rights in the code ones give forward to the downstream (customers, consumers)
PERSONAL DATA	Is any information relating to an identified or identifiable individual (data subject).

GO-DIP PROJECT: BACKGROUND AND RATIONALE

Digital Data is the new oil. Can European companies recognise the economic value of digital data intellectual property and the impacts that digital data have on business today and in the very connected future?

The digital transformation resulting from the implementation of Industry 4.0 changes the current IP management and understanding of the use of digital data. Data and algorithms using open source code increasingly serve as a foundation for the creation of added-value in the digital economy. Data is not only considered a by-product of business activities anymore, but a strategic resource that constitutes the basis for developing and offering novel digital products, services, and business models. Many of these business models will be based on the analysis and evaluation of machine-generated data. Data can be valuable in economic terms and can assure a competitive advantage to those possessing it. The European Intellectual Property Office (EUIPO) and the European Patent Office (EPO) showed in their study in 2019 that EU industries that use IP rights intensively were responsible for 45% of Gross Domestic Product, or €6.6 trillion. These industries account for 96% of EU exports and support directly or indirectly 39% of EU employment[1]. The study is pointing out that despite the evident business growth opportunities that digital data offer companies and EU economies, also face multiple challenges such as:

- Technological advancements make new distribution channels and new business models possible, but they also make it easier to infringe IPRs of digital content on the internet and/or through online sales of counterfeit goods;
- The surge in content uploaded to digital platforms raises new copyright issues with combatting counterfeiting;
- The new business models pose a challenge to both the rights holders and the authorities tasked with registering and enforcing IPRs;
- The way companies and other rights holders use IP is also evolving and becoming more complex. Firms often protect their IP using a bundle of rights, some registered (most often a mix of trade marks, patents, and registered designs), some not (e.g., copyright);
- Individually owned IPRs are sometimes supplemented with collective rights such as certification marks or protected geographical indications (GIs);
- Domain names are also crucial to brand owners and the interplay of these names with trademarks is of major importance;
- With the increasing use of artificial intelligence (AI), machine learning, and other advances in technology, the future of work is changing.

With such complexity of data-driven economies, European manufacturing SMEs do not know how to protect and monetize digital intellectual property (DIP) very well, and provide added-value using their intangible assets such as data, methodologies, configuration of interconnected systems, 3D designs, and processing algorithms. Moving towards a data-driven approach with embedded software into hardware, new questions arise concerning data-sharing, data-driven innovations, legal digital IP protection, and data ownership. These new challenges of the European digital economy hamper inbound open innovation/IP sourcing in European manufacturing SMEs.

The Go-DIP project addressed these challenges by raising awareness of digital data and software IP value, and positively the impact of IP management of manufacturing SMEs in the Alpine innovation systems and wider in the European Union area.

Valuating, monetizing data, and software IP were addressed through the use of practical cases and the direct involvement of 60 SMEs, mostly located in Slovenia, Italy, and Switzerland – the partner regions of the Go-DIP project.

In this DOP, document guidelines, templates, and cases are presented using the European Agency for SMEs' methodology, otherwise known as the "Twinning plus methodology."

Go-DiP project partners, the Jožef Stefan Institute from Slovenia, Fondazione Hub Innovazione Trentino from Italy, and Innosquare from Switzerland addressed challenges of digital economies in a survey of 26 SMEs, implementing three thematic workshops held between November 2021 and December 2021, reviewing in detail a set of legislative and strategic frameworks. Those frameworks were recently introduced in the European Union in the scope of the Digital Europe initiative and structured around the three pillars of digital IP management: Digital IP and data agreements, the legal aspects of digital IP and data management, Data-driven innovation, and exploitation.

[1] EUIPO Strategic plan 2025

The Partners

Partners in the Go DIP project come from three vibrant European Alpine regions' innovation systems with advanced digital industry – Slovenia, Italy, and Switzerland.

Jožef Stefan Institute (JSI) with Strategic Research and Innovation Partnership Factories of the Future, Slovenia
The Jožef Stefan Institute is the largest science and research institute in Ljubljana, Slovenia, conducting basic and applicative research in natural sciences, life sciences, and engineering. The Strategic Research and Innovation Partnership Factories of the Future (SRIP FoF) with technology backup from Jožef Stefan Institute is an innovation cluster with over 90 members – of which over 60 are manufacturing companies, active in ICT, robotic systems and components, intelligent control systems and management, advanced sensors, smart plasma systems, smart mechatronic tools, factories of the future, and new materials. The Jožef Stefan Institute is also a host to the Unesco Research Centre on Artificial Intelligence - IRCAI and an umbrella organisation for the Strategic Research and Innovation Partnership Smart Cities and Communities, a cluster with 140 members from research, business and academia, active in six technology areas (IoT, IoS, Cyber security, HPV, and big data, digital transformation, and GIS-T). JSI is coordinator of I4MS DIH and member of multiple digital innovation hubs including DIH for manufacturing quality.

FONDAZIONE HUB INNOVAZIONE TRENTINO, Trento, Italy
Fondazione Hub Innovazione Trentino (HIT) is a non-profit foundation founded by University of Trento, Bruno Kessler, Fondazione Edmund Mach, and Trentino Sviluppo S.P.A. Another stakeholder is the Autonomous Province of Trento. HIT has been recognised as a research and knowledge dissemination organisation according to the communication from the commission – The State Aid Framework for Research, Development, and Innovation (2014/C 198/01). HIT supports the Province in stimulating innovation in the local economic and production system, promoting dialogue and the transfer of knowledge and skills between the actors of the provincial research and innovation system, and from them to the economic and social system. HIT bridges science, technology, and business with a strong focus on managing the exploitation of IP portfolios and technologies for research industry collaborations and new ventures. Driven by regional policies on R&D and innovation, HIT supports the members in transferring knowledge and technology outside the academic environments for the benefit of social, cultural, and economic regional development. HIT is partnering with Confindustria Trento (business association) within the regional Digital Innovation Hub and leads the Smart Industry subgroup of EUSALP Action Group 2.

INNOSQUARE, Regional innovation and technology platform, Fribourg, Switzerland
INNOSQUARE is a regional innovation and technology platform located at blue FACTORY Fribourg in Switzerland. It promotes the implementation of research and innovation projects through interactions between companies, clusters, public and private entities, universities, competence centres, and research institutes.
INNOSQUARE is funded by the School of Engineering and Architecture of Fribourg, affiliated to the University of Applied Sciences and Arts Western Switzerland, (HES-SO//FR HEIA-FR) in partnership with the Economic Promotion Agency of the canton of Fribourg (FDA) and the Chamber of Commerce and Industry of the canton of Fribourg (CCIF).

The Experts

Numerous highly experienced experts in the domains of digital data management, legal protection of data, and data-based business model creation have provided valuable input to this Design Option Paper, and we thank to all of them for sharing their vast knowledge with the wider European and "global village" business and industry community in the scope of this manual. Numerous other experts were involved with sharing their knowledge during the course of the workshops which are organised around three pillars of this project, as well as during the preparation and editing of this Design Option Paper among them:

- Margherita Cera, Lawyer in Litigation and IP at Rödl&Partner;
- Elisa Toniolo IP & Innovation Advisor – Trademark and Patent Specialist Qualified Patent Information Professional (QPIP certificate);
- Andrea Fornasier, Head of DIH Alto Adriatico, Digitalization Confindustria Alto Adriatico, Product Development LEF;
- Dr. Maja Bogataj, LL.M. Founder Intellectual Property Institute, IP Lawyer & Data Ownership;
- Matija Šuklje, MLaw, Free and Open Source Software, Member of Free Software Foundation Europe;
- Aleš Veršič, Government Office for Digital Transformation, Department for Strategic Planning;
- Dr. Aleš Lipnik, Institute for Economic Research, Digital IP Innovation;
- Christophe Saam, CEO, Swiss and European Patent Attorney;

- Stefan Fischer, National Contact Point for EIC Accelerator, European Innovation Ecosystems;
- Jean-Philippe Bacher, Professor, Technology transfer responsible;
- Maud Fragnière, MLaw, Kasser Schlosser Avocats SA;
- Talia Bally, World Intellectual Property Organisation – WIPO;
- Andrea Buccoliero and Antonio Colangelo, GPI Group Trento;
- Stefan Fischer NCP SMEs, Euresearch Network Office, Bern, CH;

The objectives and executed activities

The overall objective of the Go-DIP project is to develop new "demand-driven" quality support advisory programmes/services for intermediary organisations. This was achieved through the creation of a peer learning group and developing supporting instruments and tools to assist manufacturing SMEs' digitalisation processes in the partner countries, using the European Union Twining Plus Methodology. Good governance and ethical principles for AI and data economy in accordance with the national and European strategies for digitalisation, artificial intelligence, and data economy (including recommendations of other international organisations such as the OECD Global Partnership on AI-GPAI) were addressed in the scope of the Go-DIP project, bringing closer practitioners, policy makers, businesses and research organisations.

Go-DIP in figures

Data-sharing and Data driven Innovation

- Awareness-raising of digital data IP by peer learning through cases and communication activities (i.e., six agencies, 60 SMEs directly and 100 indirectly involved, partners expressing interest in project results). The SMEs were reached through their engagement in the project survey, assessing SMEs general understanding of the digital data management issues as well as through project communication activities;
- Digital data IP validation was performed by collecting and assessing up to nine use cases which demonstrate possibilities of data IP used as revenue generators;
- Collecting up to nine use cases for the application of digital data IP in manufacturing SMEs innovation.
- IMPACT on 100 SMEs
- 9 use cases – data IP in contracts
- 9 use cases – data IP validation
- 9 use cases – data IP business strategies.

Software IP and Data IP Agreements

- Develop guidelines to properly exploit (protect and/or monetize) software IP and data IP by clarifying software licence restrictions and explore common practices in business with suppliers of tangible and intangible assets discussed with the participants of the workshops and presented in this DoP through contributions of experts and partners;
- Set up a repository of up to nine real business models/practical cases of using software IP and data IPs in contracts.
- Prepare up to three scenario-based template contracts for at least three business models of exploitation of software IP and data IP, and enforcing ownership/rights of IP exploitation in proper and fair ways, including open source data and artificial intelligence data use;
- 9 business models;
- 3 scenario-based contracts.

Data Ownership and IPR Exploitation

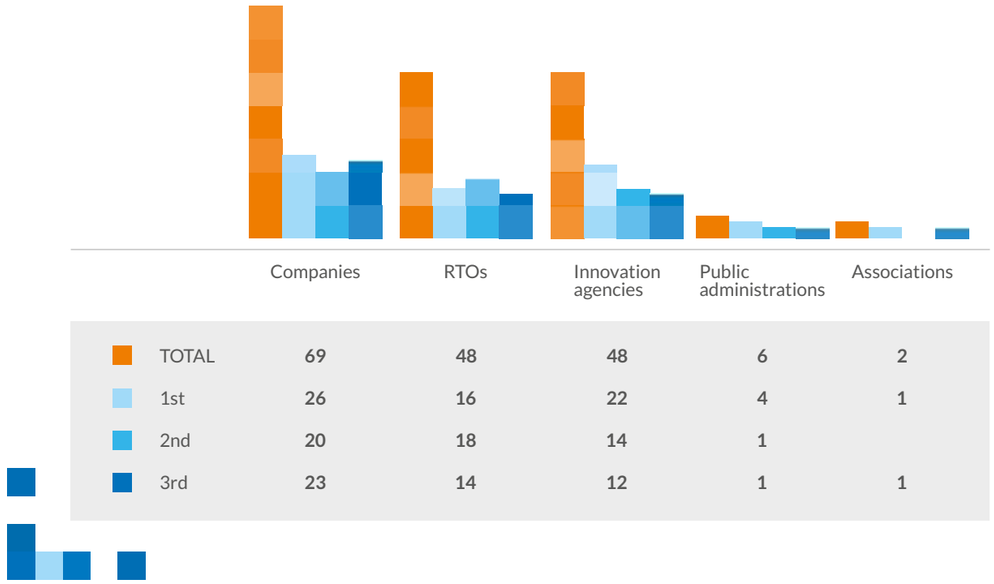
Make added value from digital IP portfolio (increase awareness of potential use of digital IP, especially digital data)

- Define up to nine various models of data ownership to raise awareness about the possibilities and options for data IP ownership exploitation
- 9 models of data ownership

Graphical representation of actual figures

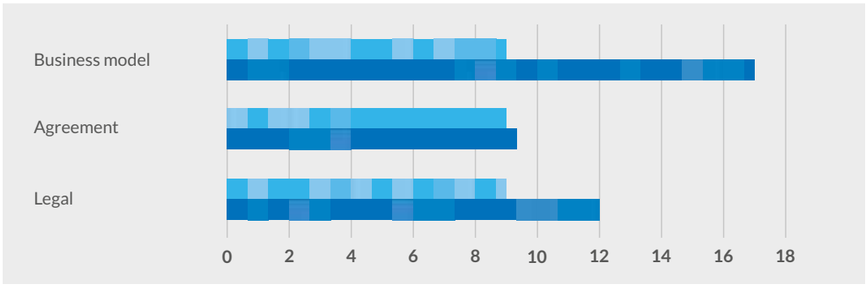
NUMBER OF UNIQUE PARTECIPANTS

NUMBER OF PARTECIPANTS



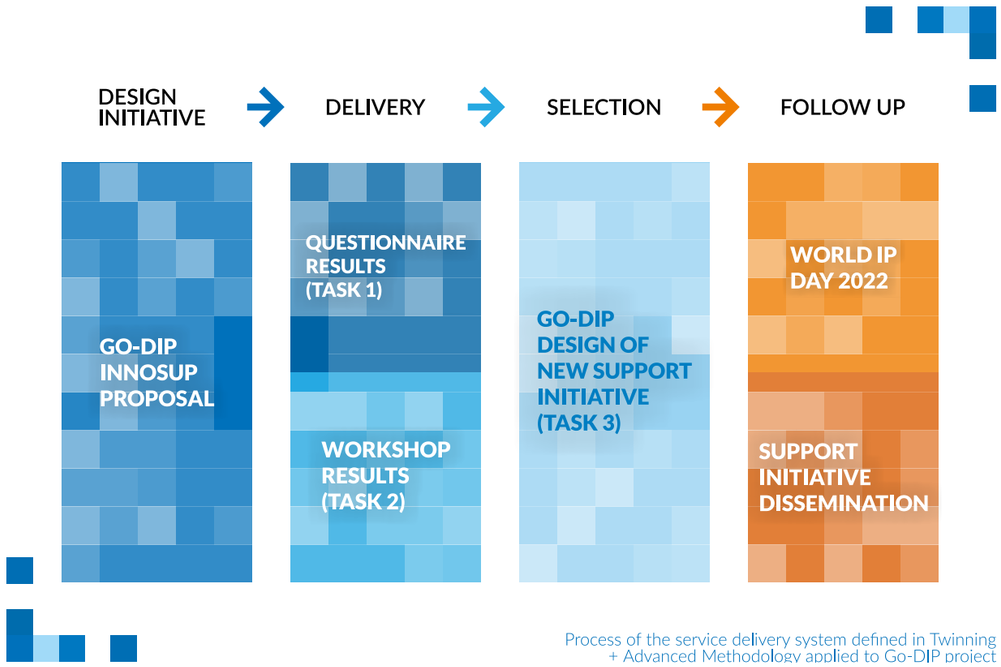
	Companies	RTOs	Innovation agencies	Public administrations	Associations
TOTAL	69	48	48	6	2
1st	26	16	22	4	1
2nd	20	18	14	1	
3rd	23	14	12	1	1

COLLECTED CASES



The methodology

The project methodology is based on the Twinning+ Advanced Methodology by exchanging existing cases, models and issues and inviting experts from the domains addressed by the project from all three participating partners. Fig.1 shows the four stages of the Go-DIP project according to the process of the service delivery system defined in Twinning+ Advanced Methodology. The first two stages, design initiative and delivery, have a converging effect towards a definition of support services for SMEs and the last two stages, selection and follow-up, have a divergent effect with the dissemination of the Go-DOP project results and of the support initiative. In this methodological framework, the work plan of the Go-DIP project was established in three tasks. Task 1 was dedicated to the collecting of challenges, experiences and good practices through questionnaire results, Task 2 was focused on three peer learning workshops and these results and finally Task 3 was about the design of new support initiatives in digital IP management.



Process of the service delivery system defined in Twinning + Advanced Methodology applied to Go-DIP project

Questionnaire results

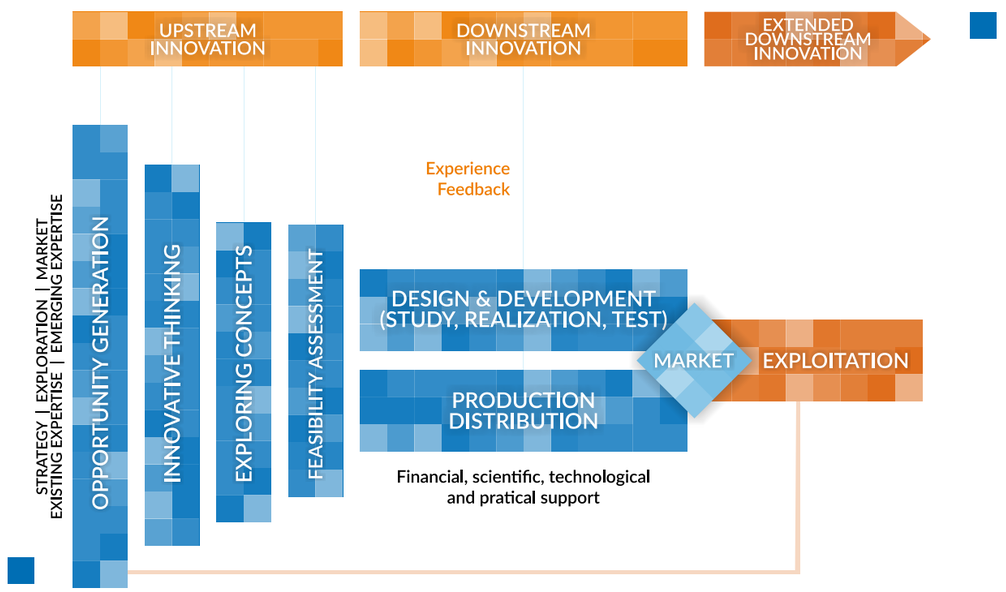
At the core of the Go-DIP project an interaction with SMEs was aspired to dive into the reality of digital transformation and engage with the real-world experience of businesses with Industry 4.0 implementation and related IP management. The involvement of SMEs was achieved through a preparatory survey and a series of workshops focusing on digital IP and data agreements, legal aspects of digital IP and data management, and data-driven innovation and exploitation.
26 companies or organisations participated in the preparatory survey, 15 of which from Switzerland, 6 from Slovenia and 5 from Italy. The survey results helped to shape the agendas for the three Go-DIP workshops by shedding light on common issues to be discussed with experts and SMEs. The participants in the survey indicated that they already have experience with digital products/services based on data exploitation. Specifically, a third of the participants has experience with AI models, 26% with sensor data and 20% with big data analytics. Nevertheless, the participants are looking for specific support in the following fields (in order of priority for the companies):

- Templates and guidelines for drafting contracts
- Understanding the value of the data portfolio and software IP
- Legal support for drafting contracts
- Knowledge on rights and obligations with respect to data usage
- Due diligence/software disclosure
- Patentability of software products

While 80% of the participants indicated that they consider IP a strategic asset, only 35% had an office or function specifically dedicated to intellectual property within the company. 75% indicated that they are not familiar with the Open Data Directive, and even 85% were unfamiliar with the European Data Spaces.

Table 1 describes the main stages of the innovation process and links them to IP and data management. Digital IP-specific aspects, as observed during the Go-DIP project, are highlighted to provide guidance for SMEs in their digitalisation process.

EXTENSION OF THE INNOVATION PROCESS OVER TIME DUE TO THE DIGITALIZATION



Generation of new innovation opportunities from big data collection and analysis

Innovation Process Tasks	*Business Tasks*	*IP Management Tasks*	*Digital IP specific*
Generate Opportunity	Pull innovation Process: Assess needs Identify technology	Analyse Stakeholders Define innovative process (Technology Pull/ Push)	Evaluate the digital-based value proposition
	Push innovation Process: Generate ideas Develop ideas		
Activate Innovative Thinking			
Explore concepts	Define structure/architecture Develop concepts	Define IP landscape	Formulate Digital IP strategic direction (multi-mode IP portfolio)
		Align Business Model strategy	Define Open System Architecture/Open Source or closed source system architecture
		Process IP development and prior art analysis	Review the digital IP current state (IP business driver)
	Perform Technology mapping	Develop IP Monitor IP Develop IP portfolio	Establish the data management plan / data sharing agreement Ensure GDPR compliance
Assess Feasibility		Get product clearance (freedom to operate)	Verify the data management plan / Data sharing agreement Verify external library licence Verify GDPR compliance
		Perform IP monitoring Maintain IP portfolio	
		Analyse IP infringement	
Design and development			
Production and distribution			
Operation	Collect big data from operations	Analyse data access	Evaluate new innovation opportunities from big data collection and analysis Establish data agreements

Workshops description

Software IP and data agreements

Topic	Software IP and data agreements
Date	November 19, 2021
Agenda	14.30–14.50 Welcome, introduction to the project 14.50–15.10 Plenary speech 15.10–16.10 Round table with best practices and cases 16.10–17.00 Workshop: Development of a checklist for model digital IP agreements
No. participants	70
Speakers	1. Margherita Cera, Lawyer at Rödl & Partner Italy with expertise in Industrial and Intellectual Property Law 2. Maja Bogataj - Intellectual Property Institute, 3. Giovanni Gaglione - Wonderflow.ai, 4. Carlo Pasqualetto - AzzurroDigitale, 5. Romana Schwab - ITG Salzburg, 6. John Whelan -Trinity College Dublin.
Main messages (quotes, pictures, etc.)	1. Databases can be protected under sui generis right only when substantial investment has been made. 2. In EU territories, software cannot be patented per se, but program-controlled manufacturing and control processes should be regarded as patentable. In this case, software provides a technical effect that is a condition enabling patentability. 3. Patent ownership and the related rights are not always immediate to assign, based on the contracts and the type of organisation, the ownership could go to the employer company, the employee or the employee could have a monetary reward for the patent filed. This strongly depends on the national law regulating work relationships. 4. Personal Data, Industrial Data, and databases have different protection strategies. Personal Data are protected by GDPR, Industrial Data can be protected by Confidentiality Agreements and Trade Secrets, Databases can be protected by sui generis Rights. 5. The innovation agencies have the role the guide companies to protect and valorize their trademark and IP, and are very effective if they are able to speak the same language. 6. The data controller who collects and manages the data can delegate part of the processing to a data processor who works on behalf of the data controller, and can do the data processing only within the scope agreed. 7. In the industry 4.0-related services, the main concerns by companies buying new technologies are related to the location of data, data breach, and freedom to operate. - Open Source is eating software. - Is is very possible to patent Machine Learning. - The value in Machine Learning is the data not the algorithm. 8. Data is what really matters; information and data are public good and cannot be protected by IPR. 9. The highest risk perceived in a TT agreement from the licensing part is related to being able to obtain the technology back in case of early termination, second is the risk to see confidential information or trade secrets disclosed to unauthorised people. The highest risk perceived from the receiving part instead is to receive claims for IPR infringements from third parties (due diligence issues). 10. The technology improvements should be regulated by the relative clause of the contract. It should be clearly stated if the improvements shall or shall not be delivered to the licensee/licensor depending on which party implemented those improvements. This clause is usually quite challenging to be agreed.

Legal aspects of digital IP and data management

Topic	Legal aspects of digital IP protection and management
Date	November 26, 2021
Agenda	14.30–14.40 Welcome and introduction to the project 14.40–15.10 Keynote 15.10–15.50 Digital IP in practice – The SME perspective 15.50–16.50 Interactive Workshop – SMEs meet the Experts 16.50–17.00 Takeaways – Recommendations to navigate current and future digital IP issues
No. participants	53
Speakers	1. Maud Fragnière, Lawyer, Kasser Schlosser avocats SA 2. Paula Reichenberg, CEO Hieronymus 3. Roger Meier, CEO ROOMZ 4. Jens Henkner, CEO CertX 5. Xavier Bays, Co-founder Swiss-SDI 6. Talia Bally, World Intellectual Property Organization – WIPO 7. Ivo Emanuilov Centre for IT & IP Law, KU Leuven
Main messages (quotes, pictures, etc.)	1. Keynote as an overview on legal aspects of digital IP protection and management - Trademarks (e.g. QoQa) - Design (e.g. the graphical interface) - Patents (e.g. method and device for identifying a data packet in a data stream) - Copyright (e.g. source code) - Trade Secrets (e.g. client list) 2. SMEs had the opportunity to discuss specific questions with the experts - How can we protect an algorithm that is sold to a customer with full modification rights? - How can we show some code to a customer without fearing that he will copy paste what we did? - Do I have IP rights when buiding an AI based on our customers data? 3. SMEs had the opportunity to apply the brand-new IP Diagnostics Tool developed by the World Intellectual Property Organization (WIPO) to concrete cases of IP processes and discuss challenges faced in the digital age with IP experts

Data-driven innovation and IPR exploitation

Topic	Data-driven Innovation and IPR Exploitation
Date	December 7, 2021
Agenda	14.30–14.50 Welcome, introduction to the project 14.50–15.20 Plenary speech with experts Matija Šuklje, Liferey Senior Counsel (https://www.liferay.com/); Aleš Veršič, MA, Ministry of Public Administration, Slovenia (www.mju.si) 15.20–16.00 Round table with best practices and cases 16.00–17.00 Workshop: State of play of data ownership and data intellectual property, assigning value to data-based innovation, evolving business model cases and templates for usage-based models, protecting AI and connected data, data spaces opportunities, and other business models.
No. participants	52
Speakers	1. Dr. Stefan Fischer NCP SMEs, Euresearch Network Office, Bern, CH 2. Leon Panjtar, CEO Salesqueze d.o.o. Slovenia 3. Miha Primožič, Project Manager DOMEL d.o.o. Slovenia 4. Dr. Radovan Sernec, R&D, Guardiaris d.o.o. Slovenia 5. Andrea Buccoliero, Project Manager R&D, Gruppo GPI, Trento, Italy
Main messages (quotes, pictures, etc.)	1. What are digital data? What kind of data spaces exist? How are data and data spaces governed in the European Union? 2. Many new EU regulations have been approved over the past few years or are under the approval in 2022/2023 that contribute to the creation of the high quality data respecting EU values and setting clear rules on data governance in the European Union, which enables the creation of high quality data. Among these are: 3. Data Governance Act, Open Data Directive, General Data Protection Regulation, Inspire Directive, Machine Directive, Free Flow of data regulation, Data Governance Regulation, Data Act, Digital Services Act, Machinery regulation, Digital Market Act and Artificial Intelligence Act (currently under preparation to be approved in 2023). 4. Issues discussed were: type of data spaces, how to create and use digital data, fair data management and use. 5. In manufacturing, there is a focus on trusted data spaces and the cooperation of companies with data use. 6. Some issues in relation to the open data: data is not free, only reuse of data is free in the public domain. 7. Creating competitive data-driven business models (DDBM) is the main challenge for companies as data affects all dimensions of business models from a value proposition, and is value-added to the revenue model. 8. A data portfolio is worth more than the sum of its parts. Companies often sell services from data processing but not the portfolio of patents or licences where they could gain significant value. 9. SMEs should think in terms of patent portfolios as a source of income. 10. Universities should create value through strategically developing patent portfolios instead of just selling the licences of patents of those who gathered the data.

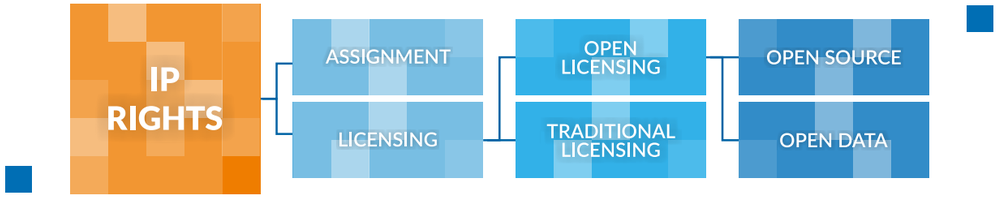
LEGAL ASPECTS OF DIGITAL IP AND DATA MANAGEMENT

IP Rights Ownership

In the manufacturing SMEs digitalization process, it is very important to consider the owner of the software created by the same company or by an external provider on behalf of the company, or that is simply used by the company according to a specific licence.

- Software created by an employee unless otherwise agreed, the employer shall be exclusively entitled to exercise all economic rights in the computer program or database created by an employee in the execution of his duties or following the instructions given by his employer.
- Software acquired by external partners
  In this case, the company will have two different alternatives:
  - 1. Acquire the copyright on software produced by external partners; or
  - 2. Use it under a licence granted by the author. The company will not be the owner of the copyright on software, but it can use it because it has obtained a licence from the software author. Depending on the company's needs, it is necessary to study the licence very carefully under which the software is released.

If the owner of intellectual property rights on software is not the company, the company should obtain a licence to use it and should respect the terms of the licence as long as it uses that software.



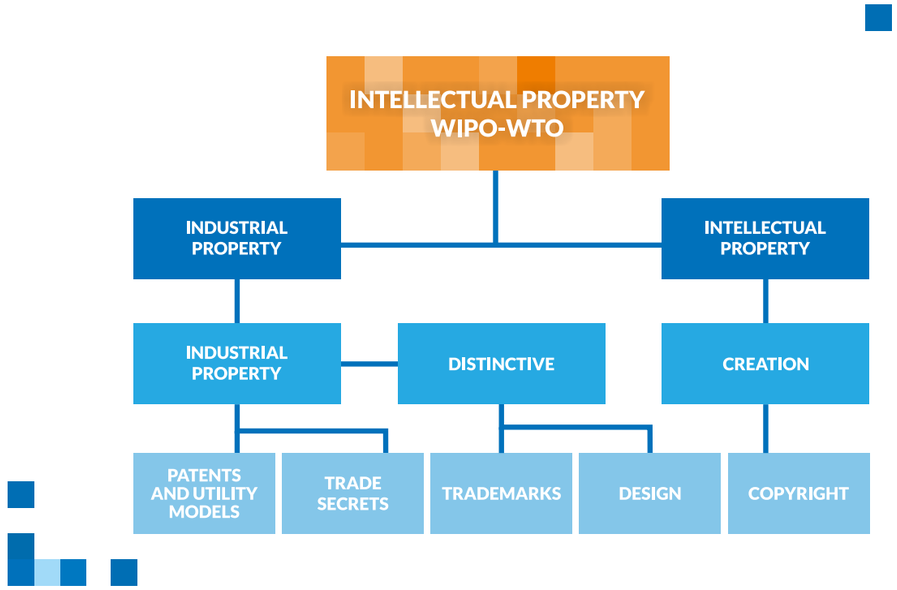
The legal framework

As an introduction, it may be pointed out that in the absence of an intellectual property right, there is no protection. Basically, in the absence of an intellectual property right, there exists the freedom to imitate. Yet, what does "intellectual property" (IP) cover?
IP may be divided into two categories: the registrable and the non-registrable rights.

- Registrable IP: trademarks, designs and patents, copyright[2]
- Not registrable IP: trade secrets.

Strategic consulting for intellectual property is very important for companies facing the digital transformation process to choose the best protection for intangible assets. Depending on the value to be protected, there are different intellectual property rights and depending on the company's market there are different territorial scopes of protection.

[2] NB: although copyright is non-registrable in Switzerland, this is not the case all over the world. For example, copyright is registrable in Italy at SIAE (Società Italiana degli Autori ed Editori), in Slovenia at AAS (Avtorska agencija za Slovenijo) and in other countries, including also the USA. Reference of registration companies from WIPO survey.



Trademarks

e.g. the well-known QOQA trademark (Swiss trademark no. 713610)

Trademarks are any word or symbol (or a combination of these) that identifies your products or services (not the company itself). Trademarks confer to their holders a monopoly on a defined territory (e.g., Swiss, EU, USA, etc.), which means that their holder can prohibit any third party to use them for the same (or similar) products or services.
The approximate costs for the registration of a trademark in Switzerland are €/CHF 1,500 – (anteriority research being excluded), including a 10 years protection. An extension for further 10 years would then only cost €/CHF 700.
One important thing that many trademark holders are not aware of is that trademarks need to be used more or less exactly as registered, in order for the protection to remain valid. Also, it is worth choosing a (as much as possible) distinctive trademark, in order for it to have a large field of protection.
By way of example, if you register a trademark with special graphism and colour, for example, but use your trademark in black and white such as in QoQa, it would not be considered a valid use and you would risk losing your trademark after five years.
In the case of infringement of your trademark, you benefit not only from civil, but also from criminal enforcement (art. 55 et seq. Trade Mark Protection Act).

Designs

e.g. design for graphical user interface: (European design DM/101 816)

Designs are visual ornamental characteristics embodied in, or applied to, an article of manufacture. Identically to trademarks, the registration of a design offers you a monopoly for a defined territory.
The approximate costs for the registration of a trademark in Switzerland are €/CHF 2,000 – (anteriority research being excluded), including five-year protection. An extension of a further five years would then only cost €/CHF 200 to 700, depending on the number of the specific designs included in your registration.
In order for a design registration to be enforceable, such a design shall be novel (which mean shall not already exist on the market) and original (must have individual character, different from what already exists). Also, it shall not have been publicly disclosed beforehand, which means that the design shall be registered prior to any commercialization.
As for trademarks, in case of infringement of your design, you benefit not only from civil, but also from criminal enforcement (art. 33 et seq. Designs Act).

Patents

e.g. "method and device for identifying a data packet in a data stream" (US patent 2 002 004 8330 A1)

Patents protect inventions of products or processes offering a new technical solution to a problem. As for trademarks and designs, the registration of a patent offers you a monopoly for a defined territory, generally for a total and maximum duration of 20 years.
The approximate costs for the registration of a patent in Switzerland are €/CHF 5,000 – (anteriority research being excluded), including the 20 years protection.
Patents are delivered for inventions applicable in industry (article 1 Patents Act). This means that computational models or mathematical algorithms, by way of example, basically are not patentable (because they are of abstract nature). However, if they are used to solve a technical problem in the technology field, they could lead to a patent, as for a neural network in a heart-monitoring apparatus for the purpose of identifying irregular heartbeats.
Patents are of particular interest in the framework of financing rounds (notably for start-ups), as they are particularly easy to valorize.
As for trademarks and designs, in case of infringement of your patent, you benefit not only from civil, but also from criminal enforcement (art. 72 et seq. Patents Act).
According to the guidelines of the European patent Convention: "A computer program claimed by itself or as a record on a carrier, is not patentable irrespective of its content.
The situation is not normally changed when the computer program is loaded into a known computer. If, however, the subject matter as claimed makes a technical contribution to the known art, patentability should not be denied merely on the grounds that a computer program is involved in its implementation. "This means for example, that program controlled machines and program controlled manufacturing and control processes should normally be regarded as patentable subject matter. It follows also that, where the claimed subject matter is concerned only with the program controlled internal working of a known computer, the subject matter could be patentable if it provides a technical effect."

Copyright

e.g. code, databases

Without needing any registration, a copyright protects you against the copy of your product. However, it does not confer any protection against products that were only inspired by your products, without being an imitation thereof.
The WIPO has issued a tool enabling you to prove the date of creation of your copyright (see WIPO PROOF).
It is recommended to always use the copyright sign ©, in relation with your proprietary rights, in order to evidence such protection towards third parties.
As for the other IP rights, in case of infringement of your copyright, you benefit not only from civil, but also from criminal enforcement (art. 61 et seq. Copyright Act).

Trade secrets

e.g. clients' data, know-how

As can be seen in the definitions and examples above, much of your IP isn't protected by registrations, e.g. data, algorithms. Therefore, it is capital to actively protect your trade secrets, which includes you, in particular your know-how.
How to actively protect trade secrets? "Best practices" have been developed, such as inter alia:

- identification of confidential information;
- limitation of access to confidential information (personal categories);
- technical measures to ensure confidentiality (tracing of access to files);
- non-disclosure agreements with penalties for employees and partners;
- non-compete clauses with employees and commercial partners.

As for all other IP rights, infringement of trade secrets can be the object or civil action (e.g., art. 321a para. 4 or art. 398 para. 1 Civil Code, or art. 9 in relation to art. 4 lit. c and 6 Unfair Competition Act), as well as criminal action (art. 23 in relation to art. 4 lit. c and 6 Unfair Competition Act or art. 162 Criminal Code). Other particular cases include:

Confidentiality Agreements (NDAs)

The confidentiality agreement is a contract by which the parties signing it undertake not to disclose the information indicated in the agreement. This agreement may be binding on both parties or on only one of them. Very often such agreements define:

- what is to be considered confidential and not subject to disclosure (e.g., know-how, financial information, unpublished patents);
- a term of validity of the agreement;
- a time limit within which the information must remain confidential;
- the consequences of disclosing the content (injunctions);
- the penalty clause whose function is to settle damages in advance.

The purpose of the confidentiality clause is to protect information which, if disclosed, could harm the interests of one or both contractual parties.
Such agreements are not valid if they are contrary to mandatory rules, public order, or morality.

In cases provided for by law, breach of the duty of confidentiality is also relevant from a criminal law point of view.

Copyright on databases

Very often, this individual data is collected on databases. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 provide the legal protection on databases, regardless of the content which could be different types of data: personal data, non-personal data, or industrial data (which can be confidential information or trade secret).
A database is a collection of information or elements, whether or not they are original works, selected and/or arranged according to criteria, or methods in such a way as to enable the user to access or consult the information individually or as a whole.
The information in the database must be presented in a certain order so that the user can find it.
The European legislator provides for a twofold protection for databases: the architecture of the database could be protected by copyright if it is an author's own intellectual creation in terms of the selection or arrangement of the material.
The author of database has the exclusive right to execute or authorise:

- permanent or temporary reproduction, in whole or in part, by any means and in any form;
- translation, adaptation, a different arrangement, and any other modification;
- any form of distribution to the public of the original or a copy of the database;
- any presentation, demonstration, communication in public, including transmission by any means and in any form;
- any reproduction, distribution, communication, presentation, or demonstration in public of the results of the operations referred to in point b).

Sui generis law on database contents

The whole content of the database, regardless of the protection of the single element or the database architecture, could be protected by the sui generis right if the database builder has suffered a relevant investment in obtaining, verifying, and presenting the content.
In this case, the database maker has the right to prevent third parties to any:

- extraction and/or
- reutilisation

of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.

The object of protection here is not the individual data, but the investment under the constitution of the database. The sui generis right is therefore granted to the person who has employed considerable human, technical, and financial resources in the systematic or methodical arrangement of information.
The creator may prohibit third parties from extracting or reusing the entire collection but may not prevent the constitution of an equivalent database if it draws on other sources independently. The sui generis right lasts for 15 years from January 1st of the year following the date of completion of the database.
The maker of the database may also decide to licence its database under an open data licence.

Personal data management

Personal data is any information that can be used to identify a living person – directly and indirectly – or that relates to them, e.g., name, location data, physical attributes, health information, economic, cultural or social identity of a person, or online identifiers.
The management of personal data in the EU is governed by General Data Protection Regulation (GDPR). Given the reformative process currently ongoing in Switzerland, tending to align Swiss law to the GDPR, it is worth applying the same principles from now on in Switzerland, too.
Pursuant to the GDPR, the general legal basis for processing data consists in having either the user's consent, or to be able to prove legitimate interests (for example in the framework of an insurance carrying its tasks), criteria which is however much stricter for sensitive data such as health data.
With regard to consent, please note that it shall be explicit (opt-in), obviously with an absolute possibility to opt-out or unsubscribe.
Also, users shall always be able to have access to their file and shall be guaranteed an absolute right to have their data deleted upon request.
When implementing your data policy, you shall be aware that the following should be drafted:

- privacy policy (which discloses the way the data is used and managed);
- cookies policy (which discloses what cookies are active);
- data protection policy (internal document providing for a plan in case of a data breach; such a document shall in particular designate the Data Protection Office, DPO, who needs to be appointed if your core activities involve processing of sensitive data on a large scale or involve a large scale, regular, and systematic monitoring of individuals. The DPO doesn't obligatorily need to be someone from your company, it can also be someone from the outside.

Also, the localisation of the servers you work with can be determinant, since the place where the data is processed/stored will have an influence on the applicable law. Generally, local or regional servers should be favoured.

Key Learning points

Special thanks to Ivo Emanuilov, Centre for IT & IP Law, KU Leuven, for his contribution to these recommendations.

Exception for text and data mining

The Copyright in the Digital Single Market Directive (CDSM) provides for an exception for text and data mining under its article 4, which covers reproductions and extractions: However, this exception is still subject to conditions that must be strictly observed. Importantly, the definition of text and data mining is so broad that it captures practically all commercially relevant analytical operations on data; In order to benefit from said exception, the following conditions must be met, all at the same time (cumulatively):

- Works and/or other subject matter must be lawfully accessible;
- Reproductions and extractions must be retained only for as long as necessary for the purpose of text and data mining;
- The exception applies only to the extent the use of works has not been 'reserved' by right holders.

Regarding the 'reservation' requirement, companies ingesting data should make sure that the data licences do not contain any such implicit or explicit reservations that may restrict the scope of permitted operations.

IP rights do not exist in a void

IP rights increasingly interact with other rights, values, and considerations that apply generally to AI. Examples include bias mitigation and automated classification and filtering that may impact access to works. Consider, for example, the situation where models trained in one jurisdiction apply certain criteria to determine what constitutes lawful use of a work. When deployed on a large scale in automated filtering applications (e.g., in the context of Article 17 CDSM) in other jurisdictions that may follow different criteria, such models could effectively limit (or unduly provide) access to works that would otherwise be considered (il)legal in the said jurisdiction.

Ownership in data

In deep learning applications, the value of the product often lies in the neural network weights. This has raised the question of whether the model should be seen merely as a database under the Database Directive, as a computer program under the Computer Programs Directive, or as some 'complex matter' in the sense of the Nintendo case where video games were characterised as such a complex matter, "comprising not only a computer program, but also graphic and sound elements, which, although encrypted in computer language, have a unique creative value which cannot be reduced to that encryption."[4]
The Database Directive extends its 'sui generis' protection to substantial investment in either the obtaining, verification, or presentation of the contents, but not to the underlying data.[5] This notwithstanding, the reality of current business practice is that many commercial models are undisclosed and access to them is provided only through an API.[6] In such cases, sharing details about the inner workings of a model with clients would usually be covered by a non-disclosure agreement.
In cases where a machine learning application is created on the basis (also) of customer data, clearing the access and processing rights, especially over personal data, requires that the data controller has legal grounds and specific purpose for processing of personal data, alongside the requirement to meet all principles of data processing established by art.5 GDPR.
The transformation of data in the process of machine learning, while allegedly considered 'fair use' under U.S. copyright law, is far from clear in an E.U. context. Companies should carefully check whether to what extent the reproduction of works would be covered by the TDM exception under the CDSM, particularly in light of problems inherent in deep learning, such as overfitting and unintended memorisation.
As far as the question of 'ownership' over data is concerned, it should be noted that the E.U. has abandoned the idea of data ownership. Data as such is excluded from the scope of protection provided by copyright law. Nevertheless, it is possible that data might still attract some protection, although not independent, when it is part of a work protected by copyright. These 'grey area' cases should be a part of any due diligence exercise.

Reverse engineering

Finally, the workshop also touched upon the question of reverse engineering of machine learning. This is a topic that needs exploration, especially in the context of security and bias mitigation of machine learning processes. Under certain conditions, legitimate interests may dictate that we need to look inside the 'black box' in order to understand how a process works and why it accounts for certain parameters and not others. While E.U. copyright law provides for a so-called decompilation exception, albeit limited to indispensable [use] to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, [7]it remains to be seen how, if at all, this exception would apply to machine learning models which are not proper computer programs.

The WIPO tool description and examples

SMEs often don't acknowledge the importance of intangible assets and commercial opportunities stemming from IP. This is particularly true, but not limited to, data-driven businesses. SMEs also often lack guidance and knowledge of the IP component in business strategy. As a response to this situation, the World Intellectual Property organisation (WIPO) developed a new IP diagnostic tool in 2021, with the specific aim to support young companies in developing their IP strategies and shedding light on certain elements that can expand their commercial opportunities. The tool was developed by the IP for Business Division with a clear business orientation, and the aim to build partnerships with companies aiming at pragmatic solutions for IP issues.
The tool is a self-evaluation tool targeting IP strategy for SMEs. By answering a series of questions on their commercial activities, users will instantly receive a personalised report based on the provided answers.
The assessment starts with a set of preliminary, general questions about the company. The rest of the questionnaire will then be adapted based on the preassessment. Overall, the diagnostic questionnaire will take approximately 1 hour and covers a total of 10 sections on the major aspects of IP rights (patents, trademarks, designs, copyrights, and trade secrets). The tool explores IP in all areas of business activity (employees, external suppliers, subcontractors, international trade, licensing, and franchising).
We encourage SMEs to take the opportunity and test the tool. It's free, flexible, and allows to respond to different scenarios for companies dealing with developing digital IP strategies:
https://www.wipo.int/ipdiagnostics/en/index.html.

Example

Within the framework of the second Go-DIP workshop organised in November 2021, SMEs had the opportunity to test the tool in real time. An in-depth case study was performed by Talia Bally, Program Support Officer at the WIPO, based on the case of a participating SME from the canton of Fribourg.
The company offers a combination of innovative

hardware (displays and sensors) and powerful SaaS software for office space, meeting rooms, and shared desk management. The company employs 21 employees, seven of whom are outside of Switzerland. It distributes its solutions in B2B through local distributors and resellers. It focuses on growing its business outside of Switzerland during the next years.
In this context, a crucial IP issue is trademarks. The company in the case-study already has a trademark for its business registered at the national level. This means that it has protected a sign that identifies and distinguishes its products and/or services from those of others in the marketplace.
The report created by the WIPO IP diagnostic tool sheds light on the value of this protection for the company in question. The trademark indeed represents a powerful business asset for the company; It prevents competitors from making unauthorised use of the trademark (that is from marketing identical or similar products under an identical or confusingly similar trademark), and it allows the company to build its brand image and reputation.
The trademark is a powerful instrument to capture the consumer's attention and make the company's solutions stand out.
However, the report created by the diagnostic tools also sheds light on potential conflictual situations for the case-study company. Indeed, it is important to remember that it is not enough to obtain protection through trademark registration.
The protection may get lost if the trademark is not properly used. A trademark may become generic if it becomes so widely used that it becomes a common name to designate the relevant good or service. In such instances, the trademark will not be registrable and a previous registration for such a trademark may be cancelled.
Also, the diagnostic tool shed light on the fact that there are companies out there with very similar registered trademarks, but active in slightly different sectors. This means that the case-study company needs to carefully analyse if its strategy to expand abroad coincides with an extension of the business into other sectors, in which case a conflictual situation might arise. A similar issue was detected at the level of registered websites.
In fact, the registered trademark is currently used for a website by another company abroad. The WIPO's recommendation is to enter into direct contact with the owners of the website before starting legal procedures to proof use and reclaim the right over the website by proofing the existence of the trademark and the fraudulent use by another company.

SOFTWARE IP AND DATA AGREEMENTS

Scenario-based agreements

SMES manufacturing companies' digitalisation process involves different players between which legally relevant contractual relationships are established.
First of all, according to open innovation business model, tools, services and assets necessaries to implement digitalization process are provided to SMES manufacturing companies by external providers which could be software houses, specialised companies, owners of specific technologies, freelancers, researchers, etc.
To this purpose, SMES manufacturing companies entered into an agreement with external providers creating mutual obligations enforceable by law.
The scope of this contract could be chosen by the parties, typically it is:

- a service agreement: software and/or App development and/or cloud computing services;
- a technology transfer agreement: assignment or licensing of know-how and other intangible assets usually protected by intellectual property rights.

To avoid SMES manufacturing companies becoming somehow dependent on providers, it is very important to provide some clauses related to intellectual property rights, ensuring the access of the source code of software and to the place where data are stored even in case of contract termination.
It could be useful for SMES manufacturing companies to adopt basically terms and conditions of services, stating the condition to which they accept to enter into a contract with an external provider.
Secondly, SMES companies entered into a contract also with the buyer of their smart products, not only by means of a traditional contract of sale, but also to regulate the terms and condition of the several Apps used by the buyer to remote control and operate the smart products. Finally, if the new technologies implemented in the smart products also allows interme-diaries, fitters, and maintenance workers to remotely control and operate the smart products thanks to the use of a dedicated App and software, then the SMES manufacturing companies should also regulate the terms and condition of such App and/or the terms and conditions of software licensing.
In all these cases the contract plays an important role for the future of the SMES manufacturing companies' business and it is very important to pay attention to its provisions.
General clauses to be provided in every contract are:

- duration,
- termination,
- applicable law,
- dispute resolution.

It should be noted that some important contractual clauses are pointed out, but the information contained in this work do not substitute a legal opinion and could not be generally applied without a deeper exam to be conducted case by case.

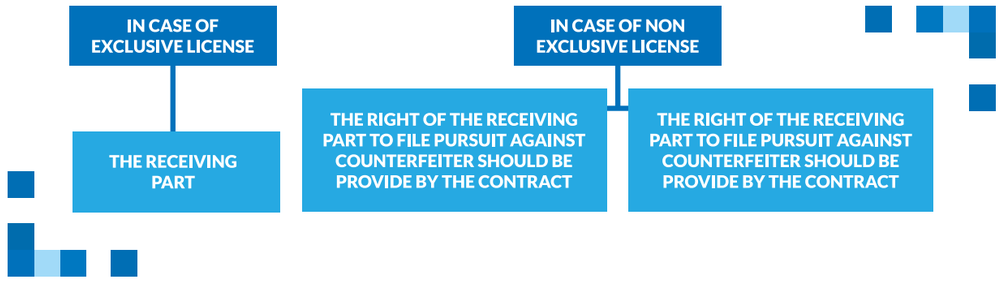
The general clauses for digital IP agreements

Price

The price should be set as an amount of money (fee) or as a percentage on the amount of sales of the product (royalties). Additional fees for technical assistance services. The best is a payment per individual service produced. It is also possible to have a forfeit.

Legal defence

If a third party infringes the IP protected, who has the right or obligation to act against a counterfeiter? If the agreement is exclusive, the receiving party could file a pursuit by default, if not differently stated in the contract. If the agreement is non-exclusive, the right should be provided explicitly and who will be in charge of the legal fee of the pursuit.



Representation and Warranties

A representation is an assertion about a fact that is true in the precise moment that the representation is made, helping the other party to agree or take other actions. The warranty instead is the promise of an indemnity if this representation is false. Examples of representation and warranties cases that could be required by licensor or licensee are:

- A request of the licensor to be indemnified and kept held harmless from and against any losses, damages, or liabilities arising from, as a result of or in connection with any claims based on industrial and commercial feasibility, usefulness, or completeness of the technology.
- The necessity of the licensee to have a representation and warranty on the existence, validity, and enforceability of the technology and of any industrial property. For the company, it is necessary to have the right to early terminate the agreement in case the technology would be considered as invalid (for example if a patent is not eligible). In the agreement, it should be taken for both of those clauses. The freedom to operate could be a support for the licensee and could be a legitimate request to the licensor.

Note1: The patent itself is no longer valid from the day of declaration of the non-validity of the patent.
Note2: When a patent is registered, it is still possible that another patent, filed shortly before, could invalidate the original patent. This can also happen after some time from the patent grant

Confidentiality

- One of the possible threats of TT contracts is about confidentiality. It is possible to insert a confidentiality clause in order to guarantee the legitimate interactions in the process without exploiting the confidentiality clause for other purposes.
- The confidentiality clause should preview a limitation in time (e.g., 5 years over the validity of the contract).
- WARNING – An error to be avoided is to provide no definition of the type and the description of which is confidential information. This could increase the difficulty in enforcing the contract in a legal cause.

An example of confidentiality clause formulation:

"Each Party shall keep the confidential information provided or disclosed by the other part in confidence and shall not disclose it to any third party except to its employees and officers who need to know such confidential information, in order to enforce the rights or perform the obligation under this Agreement or its counsel (including, but not limited to, an attorney-at-law, accountant, tax lawyer, consultant) who owes a confidential obligation for such confidential information."

"The Parties shall not use or exploit the confidential information for any purpose other than exercising their rights or performing their obligation under this Agreement."

"The confidentiality obligation under this Article shall survive for five years after the termination of this Agreement."

Early termination clause

Clauses that could interrupt the contract validity should be defined clearly. Those clauses are related to the specific case and scope of the contract, main examples of the possible domains of applicability could be:

- Lack of payment of e.g., royalties;
- Lack of training if defined in the contract;
- Breach of confidentiality as defined in the confidentiality clauses;
- Invalidity or infeasibility of the technology (Licensee fault) e.g. patent not valid in a territory.

Technology Transfer Agreements

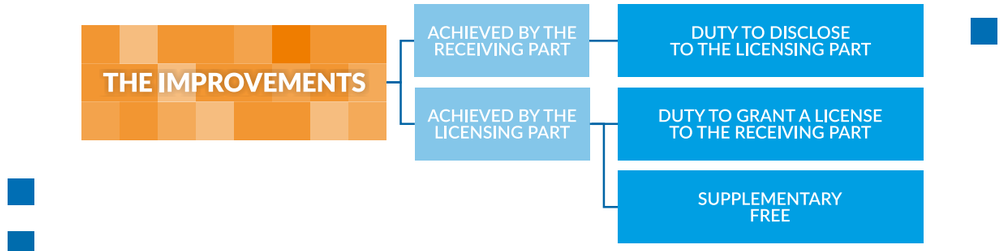
Technology transfer agreements foresee the licensing of technologies where the licensor permits the licensee (the receiving part in this case) to exploit the licensed technology for the different possible options, among which the production of goods and services for example.
The foreseen use of this type of agreement is to assign or licence to another part an IP such as registered industrial and IP rights (patents, utility models, trademarks, copyright, etc.), know-how, or technical or R&D assistance.
Possible situations where these agreements are in place could be identified in a wide spectrum of interaction from the production of goods and services where – for example – an Internet of Things (IoT) feature could be commissioned externally to an interested company or in advanced R&D activities outsourced from companies. The licensors could be – for example – universities, research institutes, single contributors, consultant companies, companies in the same supply chain, clients, or technology providers and more.
The scenarios could be synthesised into three major cases, university to business, research to business (R2B), and business to business (B2B). In all these cases, the interaction between licensor and licensee are regulated by contracts with common aspects.
For the general clauses that could be proposed in the contacts, we invite you to refer to the previous paragraph on general statement clauses.
In this section, we will follow the relevant clauses that could be included in a Technology Transfer agreement.

Training and documentation delivery

All information, documents important for the receiving party to obtain information, know-how, documentation, and data on the technology in order to evolve the technology. In everyday life, a lack of information on the use of the technology could limit and burden the technological adoption process.
In general, it is the licensor that does not transmit all the necessary information, and so it should be the licensee that requires this clause.

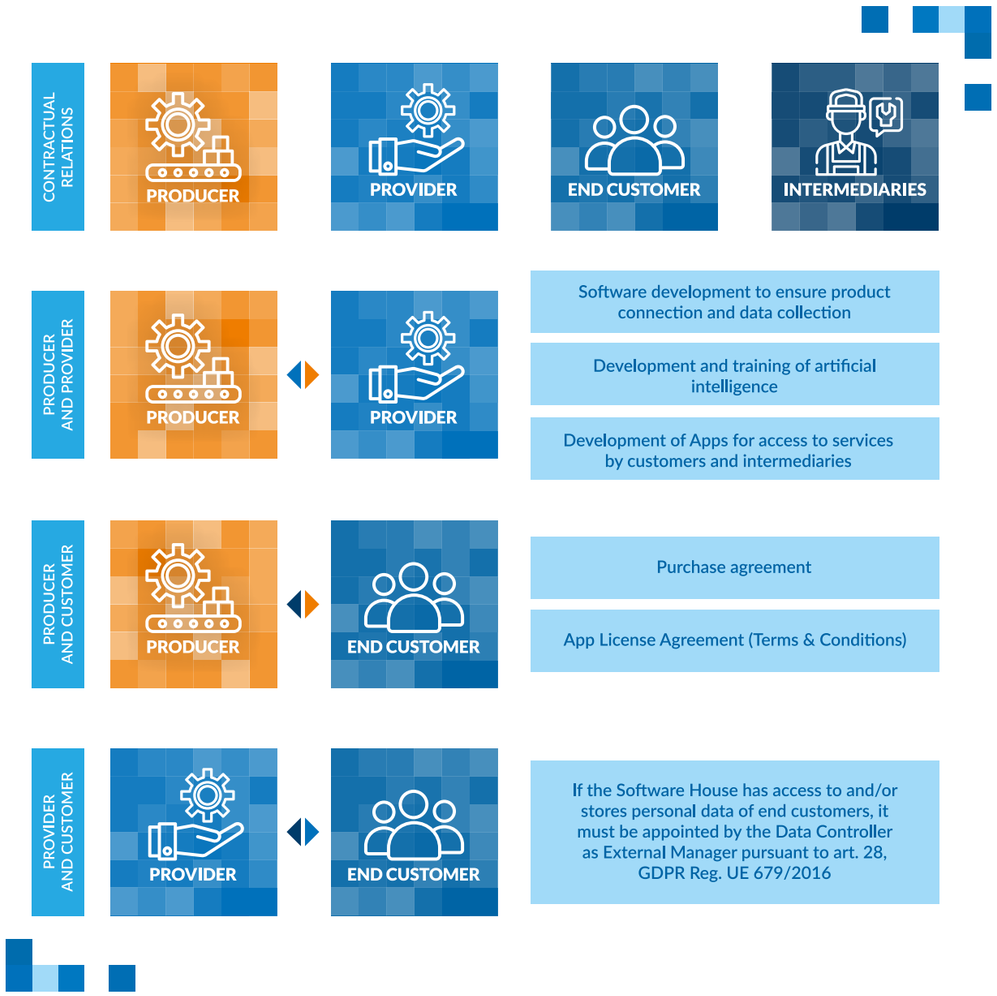
Improvement clauses

- The first aspect to be identified in preparing an improvement clause is which party will produce improvements to the technology.
- If the receiving part achieves the improvement, it is in its interest to have a protection on the know-how related to the improvement. In general, improvements beyond the licenced status are owned by the licensee. It is nevertheless possible to preview a duty-to-disclose clause to the licensing part of the improvements achieved.
- If the licensing part achieves the improvement, it is important to define the duty of the licensing part to grant a licence to the receiving part also in the improvement of the contract. Not inserting this aspect can generate a legal dispute, it is important therefore to identify an eventual supplementary fee to preview and guarantee the licence of the improvements achieved to the licensee.



The service agreements

For the service agreements, several contractual relationships may occur between producers, providers, end customers, and intermediaries.



Software and system ownership

It is important for the software provide to give a way to access the source code in order to guarantee continuity of service. If the developer becomes unavailable, this could be critical for the product owner to continue the activity.

- If the ownership is left completely to the client of the software provider, in this clause should be clearly stated an indication of the delivery of the source code to the client connected to the software ownership.
- Instead, if the software is licensed to the client, the clause could preview the option of delivery the source code of the software or to deliver the closed source binary of the software. In this second case, if the software provider fails, stops the activity, or is not available anymore to licence the software, the risk could be mitigated with an escrow agreement clause.

Escrow agreement clause

An escrow agreement clause is a clause in which one or more assets (source code, data, documents, shares, sums of money, or movable or immovable property) are deposited as security measures into the hands of an independent third party until specific conditions occur. Those assets will be moved to the indicated party if conditions that may prevent the full and proper performance of the contract occur or, in another commonly occurring case, the settlement of an international arbitration procedure happens.

Maintenance and fixes clause

If the software licensee is willing to obtain updates and improvements of the software after the software is delivered or obtain assistance from the software producer (fix identified bugs or malfunctioning), it is necessary to define the maintenance and fix clause indicating the period of validity – that should last for a period of time up to the indicated contract duration.

The data agreements

Agreements related to data should include a definition of the following points:

- Where is the data stored? In EU or outside EU?
- To whom and for what reason and how is data made accessible?
- Which is the backup strategy? Is it already in place or still needs to be implemented?
- Should the data be transferred elsewhere and in which format? Which are the protocols able to ensure and to guarantee a secure and complete transfer of the data?
- How to manage the communication safety and how to manage the data breach of the storage?

Other clauses relevant to the data management agreements include:

Personnel in charge of data management

Often the data processor company is asked to guarantee precise selection requirements and training for the personnel that will work with data in order to guarantee data security.

Appropriate measures for security

This clause should report the measures that should be put in place in order to guarantee the security of the data managed.

Subprocessors

In this clause, it should be listed if present the possible third parties or subsidiary of the main data processor contributing to the data processing. This list should be reviewed by the two parties and approved. In order to guarantee the same level of primary processor, subcontractors should comply with the same clauses of the main data agreement.

Handling of data subject rights

If the agreement is related to personal data, the data processor may be requested from the data provider itself or directly from the private citizen to manage their data according to the GDPR provisions. In this case, the data processor is the front end and there should be planned coordination strategies with the data controller.

Data breach

A specific clause should be previewed in case of loss of control of data based on a data breach. In this clause, two main aspects should be defined that are, following the standard procedures, the terms of the notification of the data breach to the data controller by the data processor and the coordination measures with the data controller to notify the public authorities, the consumers, the data owner, etc. of the data breach.

Data retention clause

In this clause, the strategy should be identified in the data management after the contract duration expires, in particular when personal data are the subject of the agreement. In general, two options could be faced, the data could be returned from the data processor

to the data controller, or the data could be deleted by the data processor. In the case the data processor is still able to access the data after the contract expiration, it configures effectively as a data breach. Other possibilities that could be agreed, could be the cession of data to the data processor or the publication of the data under an open license. This approach is extremely difficult for personal data GDPR compliance and – more in general – this must be verified for territorial law compliance.

Audit rights clause

It is important that the data controller has the right to audit the data processor at their premises in order to evaluate if the security measures and in general the contract clauses are respected. This should be indicated in the clause specifically dedicated to audit rights. It is an important element of transparency that will enable data agreement compliance.

Data transfer clause

In data agreements, it is important to indicate where data is stored and where they could be transferred. For example, if the data controller is European, the part could require that data will not be transferred outside Europe.

Data consistency clause

One clause important for the data controller sharing direct access to data is related to the preservation of the consistency of the database from the data processor. If errors occur in the data elaboration activity, or he is able to compromise the consistency of the database, the data processor could be considered responsible for the damage. With this clause, it can be requested to the data processor provide insurance for the data processor that covers the possible damage caused.

FREE AND OPEN SOURCE SOFTWARE (FOSS)

The strategic distribution of software: commercial licence or open source licence?

The distribution strategy of the software could be based on two different approaches: proprietary and open source. In both cases, the copyright owner exercises its copyright by authorising users to use the software under specific terms and conditions.
According to the proprietary approach, the copyright owner licences the software without sharing the source code, whereas, according to the open source approach, the copyright owner licences the software sharing the source code which could therefore be studied and modified by users. The chart below shows advantages and disadvantages of disclosing the source code (open) or keeping it secret (proprietary):

PROPRIETARY

- \+ IP of the owner is garanteed
- \+ Only one persona or legal entity can access and modify the software
- \+ Higher earnings for the software owners
- \- Change of owners can affect costs, functions and starting ideas
- \- May not be modified, shared, studied, redistributed or decompiled freely
- \- In the development of the software programmers do not own the rights arising from their contribution

OPEN

- \+ Minimum purchase cost
- \+ Many developers work on software development to improve the performance and make it more reliable
- \+ Flexibility
- \+ Faster identification and resolution of bugs due to the large number of developer
- \- Continous spending over time (error resolution)
- \- Development takes place without control, and is therefore more prone to malware
- \- Some technical knowledge is required for correct configuration
- \- There is no contact who can offer troubleshooting assistance
- \- Decommissioning

Choosing the most suitable type of licence is therefore of fundamental importance. The main features of open source licences are as follows:

- **Permissive:** these licences do not place any limits on redistribution and allow source code to be incorporated into proprietary software and resold within it. They may impose certain conditions such as the indication of copyright and a disclaimer in the source code and in the documentation accompanying the program.

BSD
The 4.4BSD Copyright | The FreeBSD Project

MIT

APACHE SOFTWARE FOUNDATION
Apache License, Version 2.0

- **Strong copyleft:** these licenses allow the redistribution of software, and if it has been incorporated or modified, the same conditions must be respected as for the original license.

GPL Free Software Free as in Freedom
The GNU General Public License v3.0
GNU Project
Free Software Foundation

- **Weak copyleft:** these licences allow the software to be used within other programmes that are subject to proprietary licences. Embedded software must be redistributed with its own.

LGPL Free Software Free as in Freedom
GNU Lesser General Public License v3.0
GNU Project
Free Software Foundation

Free and Open Source Software FOSS is linked to the Open Chain ISO/IEC 5230 standards relevant to the upstream suppliers and open source projects as inbound for training and policy processes, and an outbound for downstreaming to customers, users, and the community.

The FOSS compliance

Inbound licences are groups of rights (in the code). one obtains from upstreaming data from suppliers or when one downloads data. Outbound licences are the rights in the code ones give forward to the downstream (customers, consumers).
Foss implies free data as freedom. The basics of free software – every open source licence gives one the rights to use the code for whatever they want, to study the code with the source code, and to share original code with users. Why use open source? It is cheaper and tested than existing technologies, and it is used for learning and attracting talents. It can be used for learning purposes. Open source compliance/licensing compliance is a bare minimum legal requirement. Failure to follow licences can lead to copyright infringement and loss of ability to use software forever.
GPL licence breaching is an example of that.
Majority of FOSS obligations are:

- Keep licence texts and copyright notices in place;
- Keep source code and log modifications and mark your own work appropriately;
- If copyleft, resulting code has to be under the same copyleft licence;
- Look for licences that your downstream is also OK with;
- List all 3rd party code and information about it: tooling and automation helps with that.

Case: ***OpenChain – ISO/IEC 5230***
https://www.openchainproject.org/

Description:
ISO open standard for FOSS (Free & Open Source Software) licence compliance. An OpenChain certification effectively means the company has the people, policies, and processes to cover FOSS-related issues. It does not proscribe how these roles or rules should be, but does offer some examples and ample training materials. The main benefit is to produce trust in the supply chain, as if a supplier is compliant with OpenChain, its (B2B, B2C) customer can rely on that instead of doing all compliance checks themselves.

Impact on company:

- Suitable for companies of all sizes in all markets – use cases and examples are available
- Free online self-certification with extensive reference material; official service provider partners are available as well, as well as third-party qualifiers
- Text of the standard is available for free, and is developed in the open as well

Case: ***SPDX – ISO/IEC 5962***
https://spdx.org

Description:
The ISO open standard for communicating software bill of material (SBoM) information, including components, licences, copyrights, and security references. SPDX reduces redundant work by providing a common format for companies and communities to share important data, thereby streamlining and improving compliance.

- Very powerful and extensive format

Case: ***SPDX – ISO/IEC 5962***
https://spdx.org

Preferred SBoM format when it comes to FOSS license/copyright compliance

- Human and machine-readable, so also great for long-term storage
- PDX is the used for importing and exporting SBoM data – most (FOSS) license compliance tools and services can output into SPDX format, many can also import it for further processing – SPDX maintains a list of such tools
- NTIA (US National Telecommunications and Information Administration) explicitly states that SPDX meets their criteria of an SBoM, and as such compliant with the requirements of the US Executive Order on Improving the Nation's Cybersecurity
- Also maintains a list of FOSS license texts and their unique identifiers/names
- Text of the standard is available for free, and is developed in the open as well

Case: ***REUSE***
https://reuse.software

Description:
Best practices on how to properly equip your own code with appropriate copyright and license information.

- Very simple to follow steps, also includes example repositories
- Available helper and linter tools, including an API and CI integration to further simplify the process
- Minimal overhead by adding just two comment lines in each source code file
- Since it relies on a subset of SPDX, many FOSS license/copyright compliance tools understand REUSE out of the box

Main Foss compliance questions to consider are: who holds the (copy)right on the source code? Which are the applicable licences? Is the code (un)modified? How do the differently licensed pieces of code interact?

Other software and methodologies supporting the licence tracking and the FOSS compliance are depicted in the following Table:

Reuse	linter and helper tool for adding info into source code
ClearlyDefined.io	web service to check license info of packages
ScanCode	license scanner
FOSSology	license scanner with a audit-centric workflow
Ort	component analyser, license scanner, etc.
Tern	container content analyser
Bang	binary image analyser
SW 360	binds all the other info together in a coherent hub
OpossumUI	similar to SW360 but with a more light-weight approach (both in resources and workflow)

Patents in FOSS

Some of the Open Source licences include patent licences, which means if anybody who contributed to code or gives you distributed package under this licence also gives you the patents rights to use the software. This is limited only to the patents that are necessary to use this piece of the FooS. It often includes patent protection/retaliation clause. The goal of these clauses is to create a penalty so as to discourage the licensee (the user/recipient of the software) from suing the licensor (the provider/author of the software) for patent infringement by terminating the license upon the initiation of such a lawsuit. Such explicit patent licences are, for example, Apache 2.0, LGPL, GPL, AGPL. One would not be in breach of the manufacturers patents when downloading the software if you use that right on your machine. If you would start making a competitive hardware one would be in breach of the patents rights. These licences include a patent retaliation clause which means if one sues a company over a patent that you hold for a piece of software that is under Apache or GPL licence you would be the one who would lose the right to use this software from all other developers automatically. Very few licences exist that do not have anything to do with patents such as Creative Commons (CCO) 1.0. A lot of modern licences have explicit patent rights in words explained what it means. "Implied" patent licences are, for example, MIT, or BSD-3-Clause. They use patent language.

There are two networks in Europe that protect their members from patent fraud:

- **Open Innovation Network**
  - Royalty free-cross-licences for patents in FOSS packages
  - 2.7 M patents & applications
  - https://openinventionnetwork.com/
- **LOT Network**
  - License on transfer to prevent risk from patent trolls
  - 3.1 M patent assets
  - http://lotnet.com

The value of data in the Open Space and Data Governance

Data governance globally follows three different approaches:

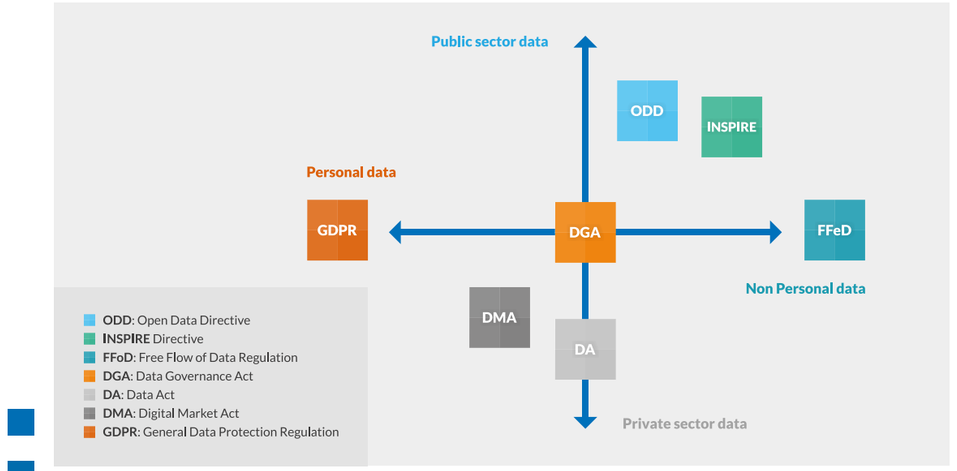
- the "Silicon valley way" (Facebook, Google, and other companies) with limited i.e. company's assigned control of personal data
- the "Chinese way" – government control of data with low protection of personal data
- the "European way" – respecting high ethical values, respecting protection of personal data, following regulations on handling data in EU.

The Open data directive dealing with managing public data is the oldest type of European governance act. It is followed by the Inspire directive dealing with the spatial data. Free flow of data is the third regulation in European Union, dealing with non-personal data. On the other spectrum are regulations dealing with personal data such as General Data Protection Regulation – GDPR. The introduction of the GDPR has had implications not only for Europe, but also globally. The newest regulations in European Union relevant for data management are the Data Governance Act and Data Act approved at the end of 2021, i.e., at the beginning of 2022, respectively. More EU regulations relevant for digital data management by SMEs are listed in Annex 1.

These data regulation acts deal also with the private sector data. The Data Governance Act regulates handling of the public sector data, i.e., the availability of public data for use by the private sector against remuneration in any form. Data-sharing intermediaries will prepare legal and other issues in relation to sharing public data with companies.

Data altruism organisations will be intermediaries between researchers, i.e., public organisations and companies enabling sharing public data under fair use by companies (for example using data from private watches to monitor public health by public institutions during the pandemic). Data cooperatives can be created by a group of SMEs to share public data.

EU LEGISLATION WITH FOCUS ON DATA



Source: Aleš Veršič , Value of data in practical way with focus on Open data; Workshop Data-driven innovation and digital IPR exploitation

Issues in relation to open data exploitation

Companies in Europe need to better understand that data generation is not free, only the reuse of data is free in the public domain.

Accessibility to the data is also an issue companies need to understand better. Ownership of the data gets complex for example: when one buys a car is the data that we use personal or not. If one rents a car who is the owner of data on personal routes as this data is produced by an individual user. Everyone has the right to use publicly available data under the same conditions. Open data directive brings new terminology, i.e., high data value set. It includes spatial data, observation data, environment, meteorological data, business data and statistical data. Access to this data is arranged through the IP institute that has to be implemented via adaptation of the EU Directives and transferred into the national legislation.

THE DIGITAL IP BASED BUSINESS MODELS

This section is dedicated to identifying and describing some business models enabled by digital IP. Those business models could leverage the company investments in digitalization to create value beyond the ones that are currently implemented in the business lines. In the following paragraphs, information on business models related to software – with a focus on cloud computing and open source – and driven by data are indicated. The last paragraph will report some strategic and organisational information to support the IP management within the companies.

The software business models

The business models based on software are extremely diverse and in continuous evolution. In the table below, we propose a summary of the most common digital business models. More details about cloud computing, data-driven, and open software business models are reported in the dedicated chapters.

Charactestics	*Description*	*Example*
Distribution		
On premises	The software is distributed locally at the client premises. Mostly used for high performance applications or to process highly sensitive data (patients' health data).	Commercial software installed on the single PC or server within the company's digital perimeter.
Cloud	The software is located on a cloud server and access is centralised.	SaaS, PaaS, StaaS (see dedicated chapter).
Speakers	Software is available in part on a cloud space and in part at the company premises.	SaaS+on premises.

Charactestics	*Description*	*Example*
Code Licensing		
Proprietary	copyright owner licence the software without sharing the source code	Office suite
Open	copyright owner licence the software and shares the source code	See dedicated chapter

Charactestics	*Description*	*Example*
Revenue streams		
Licence	copyright owner licence the software without sharing the source code	Ansys, Inventor, and more
Usage-based	The software or the service is priced based on the amount of use the client does of it.	Energy utilities
Advertising	The software contains advertising from a third party that is proposed to the end user as condition to use the software.	Google, Facebook
In app purchase	you can let your customers take advantage of a part of your product's functionality for free and ask for payment to enable additional features	Smartphone apps Amazon Music Google Play Music
Subscription	you offer your customers prepaid plans and let them sign up for using your software product for a certain amount of time or a number of users	Adobe suite Netflix
Freemium	At its core, a freemium model has a free version available to anyone, with no friction. Prompts within those free services to switch to paid subscriptions to get more volume, no advertising or more data.	WinRar Spotify
Transaction fee	The software charges an amount of money per transaction realised by the users.	ebay
Support	The software producer sells the support in terms of training, maintenance or after sale services.	Redhat
e-commerce	Electronic commerce, or eCommerce, is a business model that lets businesses and consumers make purchases or sell things online.	Amazon, Zalando
Peer to peer marketplace	A peer-to-peer marketplace is a platform where usually two sides are participating in a transaction, which can be about products (Etsy) or services (Uber, Airbnb, LinkedIn).	Uber, AirBnB, Linkedin
Ecosystem model	Ecosystem orchestrators are leveraging the customer with different services across different platforms. With the knowledge and the data, they can then upsell on existing customers and attract new ones due to the "vendor lock-in" effects their ecosystems create.	Amazon, Alibaba, Google, Apple, Tesla, GE
Revenues through data	Common ways of utilising and making money with company data include selling insights to customers, empowering the sales force with data, using data in marketing and advertising, selling data up and down the value chain, selling data outside the industry and using data to increase company valuation.	See dedicated chapter

Charactestics	*Description*	*Example*
Target audience		
B2B	The target audience in the B2B model includes business entities, who purchase and use your software product. Since such clients call for complex sales, companies will need a dedicated and trained sales team, who will be able to hold negotiations with business representatives.	Suppliers, modular producers
B2C	According to the business-to-consumer model, a software product is delivered to individual users.	Multichannel business (IKEA), internet retailers
C2C	Customer to customer (C2C) is a business model that enables customers to trade with each other, frequently in an online environment.	Etsy, craigslist, eBay

Cloud Based business models

Cloud Computing is the delivery of different services through the internet provision and use of remote storage and related services. Among the computing services offered, in addition to software, there are databases and network servers. These services are made available to the user via the Internet, which therefore allows the user to access wherever and from any device that can connect to the network.
There are various types of cloud computing described in the following section:

SaaS - Software as a Service

Software-as-a-service, so-called 'SaaS,' is a cloud computing mechanism aimed at providing software that can be used on the Internet.
The main purpose of this type of Cloud Computing is to allow the use of software anywhere, without having to download and install it on one's own PC. Consequently, the user can use the software, including all its functionalities, without occupying the memory of his PC.
The SaaS business model shifts responsibility for software applications from the author to the SaaS provider. As more and more 'Software-as-a-Service' offerings are adopted, a higher percentage of core IT systems are managed by the provider, potentially reducing risk for the author and freeing up more resources for the in-house IT department to focus on innovation and new technologies.

Consequently, SaaS solutions are mainly offered through the signing of standardised Software Sub-License Agreements for the various users who decide to sign them. This means that the user is required to sign an agreement without being able to intervene in the content of the individual clauses and having to 'adapt' to the conditions proposed by the software supplier. The user who decides to subscribe to the contract must create a personal account with a password that will enable him to access the service. Each personal account is associated with the signing of the standardised contract which allows access to SaaS for a limited period of time, generally one year.

PaaS - Platform as a Service

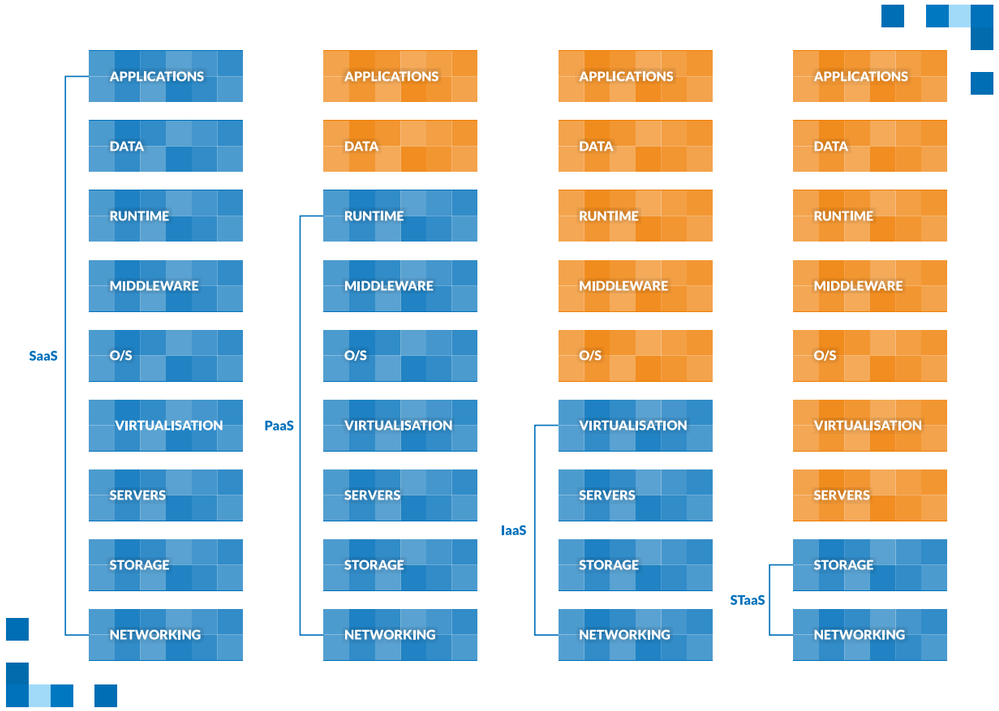
Platform-as-a-service, 'PaaS,' is a cloud computing mechanism where hardware and the related application software platform are provided by third parties. It is a service designed primarily for developers and programmers because it offers end users the opportunity to develop, run and manage an application without having to create the platform or infrastructure on their own PCs that is usually needed to carry out these activities. Indeed, in PaaS, the provider offers users the possibility of accessing its platform through an Internet connection only. PaaS is aimed at providing end users with an IT infrastructure that can be used through the Internet.
Companies typically use the PaaS model for these scenarios:

- Development framework. The PaaS model provides a framework on which developers can build to develop or customize cloud-based applications. Similar to how you create an Excel macro, a PaaS solution allows developers to create applications using integrated software components. Cloud features such as scalability, high availability, and multi-tenant capabilities are included, to reduce the amount of code developers need to write;
- Analysis or business intelligence. The tools provided as a service with a PaaS solution enable companies to analyse data and perform data mining operations, identifying in-depth information and patterns, and predicting results to improve forecasting, product design decisions, return on investment, and other business decisions;
- Additional services. PaaS solution providers can offer other services that enhance applications, such as workflow, directories, security, and scheduling.
- IaaS - Infrastructure as a Service

Infrastructure-as-a-service, or 'IaaS,' is a cloud computing mechanism aimed at providing end users with an IT infrastructure that can be used over the Internet.
With IaaS, users have the power to manage applications, data, the operating system, middleware, and runtimes, while the service provider provides the virtualisation, storage, network, and servers. In this way, the need for an on-premise data centre is eliminated, with the consequence that the end user does not have to manually perform the updating and maintenance activities necessary to use the components. IaaS is the most flexible cloud as a Service model because it allows resources, such as cloud storage, to be adapted, upgraded, and added as needed, without forcing the user to anticipate future needs and associated costs.

STaaS - Storage as a Service

Storage-as-a-Service, or 'STaaS,' is a data storage business model that allows customers to rent storage resources offered by providers through a specific subscription. In other words, it is storage made available on cloud computing that is rented from a cloud service provider and offers basic access to that storage. Small and medium-sized businesses, home offices and individuals can use the cloud for multimedia storage, data repository, data backup, and recovery and disaster recovery. There are also higher-level managed services that rely on STaaS, such as Database as a Service, where data can be written to tables hosted in CSP resources.
The main advantage of STaaS is to offload the cost and effort of managing data storage infrastructure and technology to a third-party provider. This makes it much more efficient to scale storage resources without investing in new hardware or incurring configuration costs. It is also possible to respond more quickly to changing market conditions.



Free and Open Source Software (FOSS) business models

Around the world, companies with a business model exploiting free and open source software are active and have a market share for their solutions. But, how a concept of business started with the premise of opening the source code and based on distributing the software source code free of charge can be sustainable for companies? Those companies' business models are centred around the idea that their clients are willing to pay for having something more than the software itself. The services correlated to those business models focus on customisations and new functionalities under proprietary licences, complementary services, and legal protections such as indemnification from liabilities or warranties, compliance cewrtification, or relevant services such as training, consulting, and technical support. The major benefits for the companies willing to use the open source software are possible, first among them the possibility to strongly limit the risk of lock-in with a software provider and therefore to be at the mercy of evolutions in pricing policies and commercial strategies. Further information and references on the FOSS will be reported in the dedicated chapter of this Design Option Paper.

Approaches for businesses based on FOSS

Not selling code	**Professional Services** such as training, techincal support and consulting
	Branded Merchandise like t-shirts and mugs
	Software as a Service is a way of delivering applications over the internet - as a service. Instead of installing and maintaining software
	Crowdsourcing is a type of participative online activity in which an individual, to a group of individuals, the voluntary undertaking of a task via a flexible open call
Selling users	**Partnership with funding organizations** governments, universities, companies, and non-governmental organizations may develop internally or hire a contractor for custom in-house modifications, then release the code under an open-source license.
	Advertising-supported software generates revenue for its developer by automatically generating online advertisements in the user interface of the software on a screen presented to the user during the installation process.
Selling IP	**Dual licensing or open core** in a dual licensing model, the vendor develops software and offers it under an open-source license but also under separate propriety license terms.
	Selling certificate and use of trademark franchising
	Re-licensing under a proprietary license if a software product uses only own software and open-source software under a permissive free software license, a company can re-license the resulting software product under a propriety license and sell the product under a propriety license and sell the product without the source code or software freedoms.
Selling proprietary additives	**Selling optionalextensions** such as modules, plugins or add-ons **Selling required proprietary parts** keeping of required data content (for instance a video game's audio, graphic's audio, graphic and other art assets) of a software product proprietary while making the software's source code open-source. **Selling proprietary updates** Note: this practice does not conform with the free software principles as espoused by the FSF **Selling without proprietary licenses**

Data-driven business models (DDBM)

Creating competitive data-driven business models (DDBM) is the main challenge for companies as data is affecting all dimensions of business models from value proposition to value added to the revenue model.
Data is becoming a key resource not only for processes, but also for business models. With the adoption of new technologies, the amount of data is growing exponentially. This is particularly true when referring to Industry 4.0 and the corresponding paradigms.
New technologies are providing more and more opportunities for generation of massive amounts of data via different sensors for different purposes. The core activities of DDBM become data acquisition, data evaluation, and/or data use.
This new and different data solutions (i.e., monitoring, diagnosis, adjustment, optimisation, predictions, etc.) mean new value proposition and value-added, and becomes the core element of any company business model.
Crucial questions today are:

How can we use technologies (and new data obtained) to deliver data-driven services and create new business models?
Fast technological developments and changes require continuous monitoring and evaluation of existing technological possibilities related to DDBM. As a result of this monitoring, quick response regarding implementation of new data-driven services or improvement of existing services is needed.

What is the value of my data? Can I generate revenues with data? Is my data sensitive and in which form?
Shift from non-data to a data-centric view represents a major driver of the digital transformation. Regardless of the value proposition and value-added, focus on data affects all segments of existing business (company culture, processes, resources, costs, revenue, or services portfolio).

Issues to consider with developments in DDBMs regulations

Fast technological developments and changes affect present IP management practices in many ways and the overall framework is changing over time.
Current challenges for global policy makers and organisations like WIPO are:

- To define appropriate and legitimate practices with respect to the collection, storage and use of data;
- To identify what restrictions are appropriate for the collection and subsequent use of data, we need to understand why these restrictions are necessary;

- Exceptionally powerful means of collecting data of all types (e.g., voice, text, image, etc.) exist, we still need to identify appropriate means of collecting and using those data.

Legal and policy factors coming into play when establishing possible business operating frameworks are:

- Privacy (GDPR, Declaration of Human rights);
- Security (restrictions);
- Taxation (How to track transactions, who has the right to tax, etc.);
- Property of data and intellectual property. Currently trade secrets are the dominant means of protecting the (unpublished) data in the digital economy.

Examples of Data-driven Business Models

The following table defines six DDBM that currently see an application in the market and are listed in a growing order of complexity and aperture from single product level to complex network levels.

Data-driven Business model	*Description*	*Example BM*	*Example companies*
Product innovator	Data is exploited to guarantee new functionalities to the single product.	Optimal configuration of devices IoT company – app-based product	Fed-ex Tesco Whirpool AzzurroDigitale
System innovator	Data is exploited to guarantee new functionality to related sets of products that are interconnected and generating interrelated data	Remote control Domotics Alarm systems	Honeywell process control Emerson Network Power Energenius
Data Provider	Data is generated in the company and the datasets are then commercialised for third party use and purposes.	Sectoral analysis Open data aggregation in datasets Public sector data extrapolation Process or machine data	Airbyte EcoSteer
Data Broker	Data is collected and aggregated by the company that commercialised composite datasets for third party use.	Marketing Fraud detection Risk reduction	Treato.com chino.it
Value chain integrator	Data is valorized by the company by addressing value chains problems and deploy solutions that interpret the data to give further added value to the clients	Online/offline maps services with traffic data/etc. Energetic balance and efficiency optimisation Optimal material use and track of the warehouses.	PepsiCo TomTOm Apple Wonderflow
Delivery network collaborators	Data is valorized by the company using it to manage broad networks of clients that may be both private, public, or physical persons.	Online stores Multipurpose online services On Demand services	Amazon Netflix

Organisation models and strategies for IP management in companies

Organisations can implement in their structure an IP management strategy. Organisational structures, including IP management groups, can improve the management of the IP from the early phase and can imply two main consequences: firstly, an enhancement of the competitiveness of the company by enforcing the rights connected to the IP; secondly, it can take advantage of the due diligence processes and avoid legal consequences for the infringement of others IP rights.
The main strategies for the IP protection, in particular for the protection of the digital IP for processes/products and for the company data, can be declined based on several approaches.

- **Defensive approach** – protecting the IP produced from the company business implementation is beneficial to protect the competitiveness of the products and to prevent counterfeiting. In order to pursue this strategy it is necessary to preview a budget for the IP protection and the eventual enforcement of the IPR with legal actions.
- **Aggressive approach** – the IP protection is executed in order to avoid competitors to reach new technologies that could improve their product quality, reach the technological level of the company, and therefore address the market at a higher level of competitiveness.
- **Differentiation approach** – with this approach the company can exploit the IP to enter new businesses or new markets. By protecting the IP in the company, extending the territorial coverage or acquiring the IP rights from third parties, it is possible to prepare the access to the "new to the company" markets and gain rapidly market quotas in an effective way.
- **Exclusion approach** – the approach supports the company business protection by avoiding that other companies could enter the market segment focus of the business line(s) for the organisation. This could refer to the IP generated during the organisation's product development, but also the extension of the IP protection in other territories.
- **Monetization potential approach** – the IP of the company is one of the core assets of the company. If adequately protected the IP adds value to the company increasing the attractiveness for investors, and enables potential revenue streams by licensing or cession of the IP to third parties. The IP acquisition and exploitation is per se a market that sees several potential buyers and sellers. This is true in particular for innovative technologies and digital IP.

To manage the IP generated by the different business lines of the company, it is necessary to identify roles and responsibility in the company. From a 2015 project done by IPO (Intellectual Property Owners Association), and based on interviews to 20 private companies, emerged the following considerations[1]:

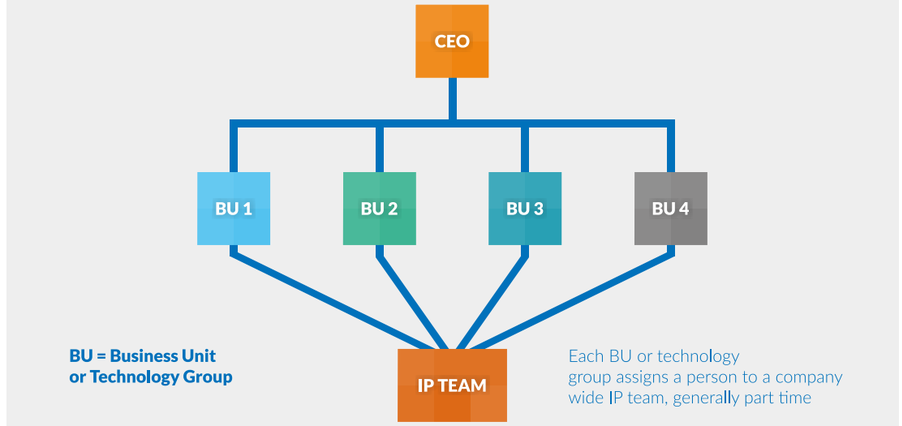
- Most companies have an executive committee that determines overall IP strategy, priorities, and budgets. This group typically includes a patent review committee made up of IP attorneys, executives, business unit managers, and R&D managers. These committees use invention disclosure forms to make decisions on patentable inventions or trade secrets;
- A majority of those companies set budgets once per year. These budgets are normally prioritised based on technology outlook and overall company budgets. Some companies' budget litigation and IPR work separately from IP management and prosecution work to account for unpredictability in litigation costs;
- The majority of companies used outside specialists for patent prosecution, IP valuation, and tech transfer activities. Outside counsel prosecution work accounted for between 50% and 90% of company prosecution activities.

Based on the dimensions of each company the groups working on the IP management could vary in composition and complexity. Some organisational structures examples are described in an article on the Journal of Technology Transfer (2008)[2] :

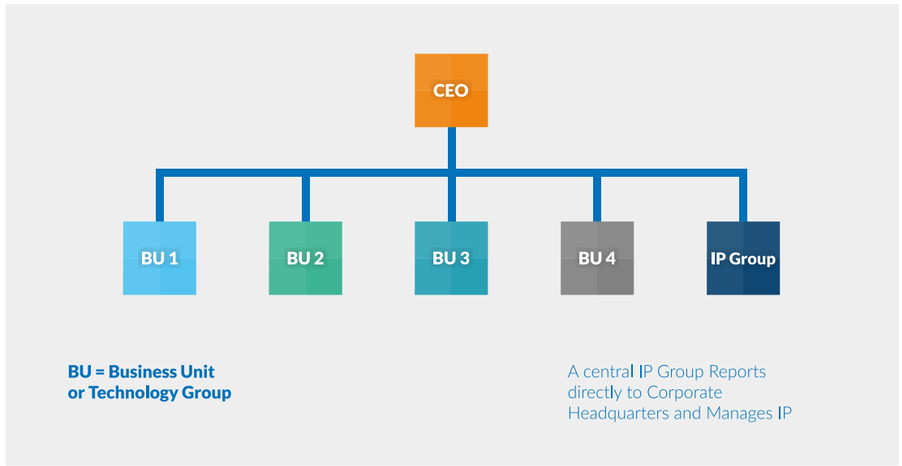
- Business Unit (BU) Assignment Model – in this model, each Business Unit (BU) identifies a representative reference for the BU that collaborates with the activity of a company-wide IP Group. This model should support companies where IP is a strategic asset, but whose IP is not easily detected in common processes. This can happen in the vertically organised company with a relevant number of levels nested under the BUs.

[1] IPO Corporate IP Management Practices Project - 2015

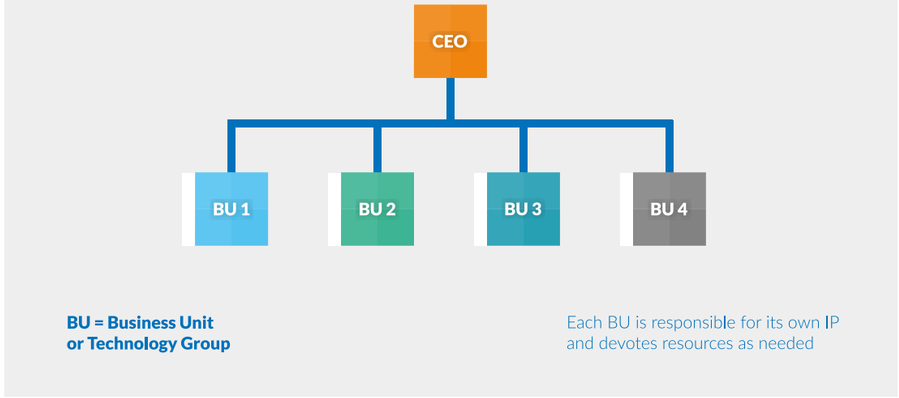
[2] Intellectual property (IP) management: Organisational processes and structures, and the role of IP donations - Journal of Technology Transfer - January 2008



- Centralised IP Model – for this model, the IP Group acts separately from the business units (BU) and is efficient when the Company IP is easy to identify, and on the other hand, when possible complexity in management of licensing, litigation, or IP protection are frequent in the company activities. This model is characterised by a high fixed cost and so could be adapted to highly innovative companies or companies working on new technologies where IP is the foundation of the business.



- Decentralised IP Model – this model is completely decentralised, the business units (BU) are directly responsible for the IP they generate, and may be exploitable in companies where the necessity to leverage IP is less demanding and the IP identified is not representing a high complexity level or interconnection between BUs. This model could therefore better suit small companies with a reduced organisational complexity and characterised by a low to medium innovation level.



An important aspect is the engagement of the employees in the IP management process to leverage the attention to the IP identification, and so the IP disclosure to the decision-making levels of the company.

STRATEGIC HINTS

- Be aware of the IP rights which can protect your intngible asset checking if all the requirement for the protection are fulfilled to be ready to react to any form of counterfeiting and to evalutate all the possible fisical implication
- File the application for the necessary registration and chose the territories to be covered by registration according to the best strategy, in this way you can stand out in the market and be recognised by consumers, rise the company competitiveness, acquire new market shares, integrate new business models based on licencing and rights
- Define a budget for IP management dedicated for activities such as prior art investigation, patentability check and freedom to operate analysis, IP protection costs, legal prosecution but also training on IP management and investments to protect the IP in the organisation
- Check the employee contracts and the agreement with the external provider to verify if the standard IP clauses are provided to the benefit of to company
- Monitor and protect your trade secret by exploiting confidentiality agreements, avoiding IP leak from unaware/unloyal employees, track and keep the timing of the newly created IP
- Always contact experts in the field (such as patent attorneys or lawyers) to avoid making mistakes

Getting Value from a Patent Portfolio

A patent portfolio has a monetary value, but it can only be monetized if there is a simple licensing business model like licensing, selling parts or all the entire portfolio, and equipping organisations with valuable IP.
Because of the large number of patents, a patent cannot be circumvented. Even if a number of patents expire, are declared invalid or become obsolete, a patent portfolio can keep its value when properly maintained and managed. Things to keep in mind when planning an IP protection based on patents are:

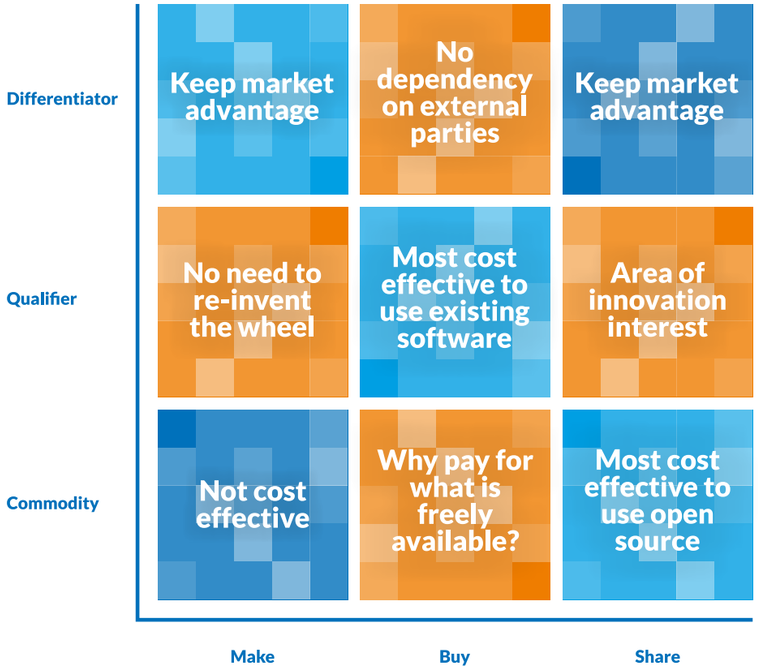
- Only very few patents are valuable,
- We never know which patents will end up being big winners,
- Insurance companies routinely deal with low probabilities of high-payout events,
- Trying to sell individual patents is a waste of time,
- Choose a growth industry,
- Patent portfolio should cover an entire value chain,
- Develop a suitable business for the licences,
- Establish a licensing sales channel.

By investing in a patent portfolio, its value can be increased through:

- The purchase of patents,
- Development of in-house inventions,
- The commissioning of contract inventions,
- Licence agreements.

How to choose the right approach to follow? It depends on the value of the IP generated that can be a commodity, a qualifier, or differentiator. The following map can help the orienteer in the decision-making process.

THE MAKE/BUY/SHARE DECISION MATRIX



The 3D printing revolution

What was the reason of the sudden hype for 3D printing in 2015?

- Critical 3D printing patent expired between 2013 and 2015 that allowed people to build 3D printers and bring them to the markets.
- At this time, 3D printing technology was already more than 10-years-old, but patents were privately owned and it was impossible for small companies to acquire licences for critical patents from a large number of licence holders.
- There was no market place for a comprehensive licence package.

So, patent owners were not able to create a significant income from their patent

The Complexity of the MPEG-4 Video Compression Standard

If you watched video in your browser recently, it is likely you have used the MPEG-4 compression standard. MPEG-4 is a video compression standard developed by a consortium of companies. Companies today would not be able to negotiate licences with each individual company contributing to the MPEG-4?

- MPEG LA was founded to address the biggest challenge to adoption of the MPEG-2 codec: the efficient access to essential patents owned by many patent owners.
- MPEG LA licences patent pools covering essential patents required for use of the MPEG-2, MPEG-4, IEEE 1394, VC-1, ATSC, MVC, MPEG-2 Systems, AVC/H.264 and HEVC and DisplayPort standards.
- Example: DisplayPort licence which is USD 0.20 per DisplayPort product.

Hard disk patents

Georg Papst had to sell the company his father had founded, the apst-Motoren GmbH & Co., and he did what nobody understood: He bought back the entire patent portfolio. Because he knew their value. I founded PAPST LICENSING GmbH, which in 1993 acquired the patent portfolio of Papst-Motoren GmbH & Co. KG of approximately 600 patents and patent applications. Therefrom Georg Papst established a worldwide operating patent licensing company specialised in the monetization of infringed patents. He then relentlessly requested licences from all hard disk manufacturers who – without exception – needed to use the patented technology and enforced his right by all legal means

ACTORS SUPPORTING AND PROMOTING THE IP MANAGEMENT FOR COMPANIES

IN THE COMPANY

- Inventors/authors: employee contributing to the company's know-how, invention and creative works
- Legal office: it is responsible for protecting the legal interests of the company in general and it provides a first general legal advice and assistance to the company on issue related to commercial law, labour law, IP, privacy...
- Company IP teams: group of IP specialist in charge to evaluate the best Ip protection strategy, to file application for IP Rights registratio) and to keep contact with external consultants
- Cyber security specialist: employee, that deals with the security of trade secrets

EXTERNAL CONSULTANTS

- Inventors/authors: external providers contributing to the company's know-how, invention and creative works
- Lawyers specialised in IP: consultants that can help the company in choosing the best strategy to protect the intangible asset, in filieng trademark or design registrations, in enforcing the IP before the jurisdiction, in drafting or reviewing IP Contracts
- Patent attorney and trademark agent: consultants that can help the company in choosing the best Strategy to protect IP, in filing patents, trademark and design registration
- Tax advisor and financial advisor: consultants that can help company in evaluating the intagible asset for tax or commercial purposes in finding financing for the R&D activities or for the IP cost of protection

[5] https://apache.org/licenses/LICENSE-2.0#patent
[6] Christopher Moran, "Machine Learning, Ethics, and Open Source Licensing (Part II/II)", The Gradient, 2021.

NATIONAL AND INTERNATIONAL ORGANIZATIONS THAT SUPPORT IP ANAGEMENT

- National Offices: Most of the countries have their own competent national office which deals with administrative activities of registration and granting of national trademark, design and patents: a list of competent national office can be found here. In Italy for example we can find the UIBM (Ufficio Italiano Brevetti e Marchi), an office of the Ministero dello Sviluppo Economico (MISE)
- Copyright Registration and Deposit Systems: Most of the countries have its own competent national office. For example in Italy SIAE (Società italiana Autori ed Editori) is a society established for the copyright protection of authors and publishers
- EUIPO (European Union Intellectual Property Office): european office dealing with trademark and design registration, guaranteeing protection throughout the european union with a single application;
- EPO (European Patent Office): European office dealing with patents
- WIPO (World Intellectual Property Organization): is the global forum for intellectual property (IP) services, policy, information and cooperation

NATIONAL AND INTERNATIONAL ORGANIZATIONS THAT SUPPORT IP ENFORCEMENT

- National and international organizations that support IP Management (see previous box)
- Jurisdictional authorities: Court and Tribuanal to which recourse can be had for the protection of the IP rights
- European Observatory on Infringements of Intellectual Property Rights: network of experts and specialist stakeholders that brings together representatives from EU bodies, authorities in EU countries, businesses and civil society, whose aim is to improve the fight against counterfeiting and piracy by sharing information and best practice, raising public awareness, strengthening cooperation, and developing better tools
- Memorandum of understanding on online advertising and IPR: is a voluntary agreement facilitated by the European Commission to limit advertising on websites and mobile applications that infringe copyright or disseminate counterfeit goods
- Memorandum of understanding on the sale of counterfeit goods on the Internet: is a voluntary agreement facilitated by the European Commission to prevent offers of counterfeit goods from appearing online marketplaces

FAQ

Personal data

Is there a risk that GDPR will put the EU in a less competitive position versus the US by putting restrictions on sharing of 'sensitive' human data (e.g., human neuroimaging studies)? Will this reduce the ability to share data in the EU for purposes of developing AI?

Indeed, the GDPR is putting EUROPE in a more advantageous position since it is becoming a global standard.

If we analyse personal data for a client, is this client the part who needs to ask for people's consent? What kind of proof of consent from the natural person should we ask for from his part?

You don't need to verify each step. Instead, it would be better to include confirmation in the data analysis contract, this is an important topic that could owe you the required compliance.

What about medical data, is there any obligation to make this data free for the benefit of society thinking in particular to personalised medicine etc.?

Medical data is a prime example of personal data – you need to make sure this data is properly anonymised.

Is data managed by the Human Resources departments considered as personal data in the same spirit as customer's data? (employee working hours, days off, etc.)

Yes.

Licences

What kind of licence do you suggest to apply in order to increase the value of the software?

There is no immediate answer. It depends on what you consider as "value." If value is to maximise the amount of money for which you can sell your company to a venture capitalist or in an initial public offering, the answer is quite different from if value is earning money from selling software licences, earning money from offering services, creating an ecosystem around your software or finally maximise the use of your technology (e.g., standardisation).

If a technology is protected by a patent, how can I licence it: worldwide or only in the territories where the patent has been obtained?

You can licence it with different kinds of contract: technology transfer or licence. The owner of the patent can allow third parties to use the technology within a special territory, in an exclusive manner or not, after a payment or not.

As long as you own the patent (or a broad enough licence to it), you can give a world-wide licence. In practice it will apply only to those territories the patent is valid in. But for those territories where the patent is not in force, the recipient does not need a patent licence anyway, so the fact that you cannot give them a patent licence for that territory changes nothing on their end. See, e.g., how Apache Foundation includes a patent licence in its Apache-2.0 software licence – most contributors in most software under Apache-2.0 do not hold relevant patents, let alone for all the territories Apache software is used in, yet the patent licence is there[5]. A wise choice is to consult a patent attorney in this case.

When you have open source and a spin out - what do you actually licence to spinout?

In this case, it is possible to licence the software copyright to the spin-out starting from the hypothesis that the research institution owns the IP and therefore the copyright. However it is recommended to specifically ask permission for the copyright owner to be licensed as open source software. Essentially, it is possible, the researcher must ask for permission, but approval depends also on how the project was funded so the question should be clarified on a case by case basis. Also, if the licensee is a campus company (spin out) we must be confident that the company is the right vehicle and has sufficient capital and the right team to exploit the software to create economic and social impact.

Artificial intelligence

What about the IP of software generated by Artificial Intelligence?

AI can be inventor or author, but the European code has denied that the machine can be inventor.

Our legal system doesn't recognize the right to the machine. The owner of the software can exploit the invention.

Do we have the IP rights when building AI based on our customers' data?

Output data belongs to the company that has implemented the AI. Including Privacy policy implications. Strong contracts are needed and legal consultancy is strongly advised.

Can data generated by Artificial Intelligence be protected[6]?

In the new EPO Guidelines, AI inventions fall under the general rules for patentability of mathematical methods (G-II, 3.3). The examination approaches for AI/ML inventions are similar to the "two-hurdle approach" for patentability of CII. The updates lay out how to overcome technicality hurdles and provide multiple examples.
An AI invention with a technical character fulfils requirements under Art. 52(2)(c) EPC. The claimed subject matter must be directed to a technical device having an inherent technical character (i.e., computer, processor) or a method involving the use of such technical means. For AI/ML inventions, the first (eligibility) hurdle can be overcome by formulating the claims as established for CII.
Further, if novelty is established, examiners assess whether the claimed subject matter is inventive. To assess inventiveness, the features that contribute to the technical character are taken into account. Thus, AI/ML inventions must demonstrate that the claimed subject matter serves a technical purpose.

How do you protect an algorithm?

The answer to this question depends on clarifying, legally and technically, what said 'algorithm' comprises. Traditionally, in machine learning there are (at least) two ways to describe algorithms. First, an algorithm could refer to the software system that makes predictions based on input data. This is also referred to as a 'predictor.' Second, an algorithm could refer to a software system that adapts some internal parameters of the predictor in such a way that it performs well on future unseen/new data. In this sense, an algorithm concerns adaptation as meaning 'training of a system'.[3]

In a legal agreement concerning the sale of provision of access to such 'algorithms,' it must be clearly stipulated what exactly is covered by said 'algorithm.' This is a challenge of both technical and legal nature. AI is based on computational models and mathematical algorithms which are per se of an abstract nature. Nevertheless, patents may be granted when AI leaves the abstract realm by applying it to solve a technical problem in a field of technology. For example, the use of a neural network in a heart-monitoring apparatus for the purpose of identifying irregular heartbeats makes a technical contribution. The classification of digital images, videos, audio, or speech signals based on low-level features (e.g., edges or pixel attributes for images) are other typical technical applications of AI. Further examples are listed in the Guidelines for Examination in the EPO, G-II, 3.3 Mathematical methods.

Data mining

So if data is publicly available, we are free to use it?

Data cannot be considered as a single IP with uniform characteristics. According to the digital single market directive you can use publicly available data if your work is lawfully accessible. A lot of public data available on permissive licence types.

Are we allowed to scrape data from websites and make business with that data?

Data is not protected by copyright. Infringement occurs if you copy an artwork but not if you are using that data for example to train algorithms.

Software and data Ownership

If a software is developed by more than one person (particularly many researchers with different contract typology), how can I identify who owns the relative rights?

The software belongs to all persons if originated by a collective work, it is fundamental to regulate the ownership with the contract even before the research starts.

FAQ

Who has the copyright on translation?

Translations are a derivative work. To use the original text for the translation you need the approval of the owner of the original work.

Who owns which data?

The data that is the result of an AI process belongs to the company who created AI. Considering the novelty of the subject it is imperative to have clear and strong contracts.

What must be considered confidential and why? Is it possible to anonymize data to make it exploitable?

The reference for this topic is the EU data protection regulation. If data is publicly available they are not confidential any more.

Litigation

The same name is used in app names in the Apple store. Can we ask to change if trademark application is refused?

You can initiate civil proceedings, but it may cost several hundred of thousand euros. First try with an official request to change the name.

Another company with the same name. What can/should we do to protect our IP?

The best strategy is filing an opposition, it is an alternative characterised by a quite low cost with respect to file a civil proceeding.

If I am the owner of all or a part of a software/data, how do I claim my right against whoever is using the software/data?

You should file a pursuit with the judicial authority in order to obtain provisional measures to stop the counterfeiter or file an ordinary judgement to obtain damages recognized.

Agreements

You mentioned that penalties are very important to be included in a NDA, but they are very difficult to negotiate with a Partner. Would injunctive relief be a better option in order to try to reduce the damage as much as possible?

The first thing is nevertheless to try to negotiate penalties. In case, you can initiate an injunctive procedure (civil proceeding, so quite expensive in the range of 40K–50KE)

How do you secure the best trustworthiness of digital data protection? What kind of risks mitigating points/clauses in contracts can you outline to limit/minimise/prevent data exposure of confidential data?

An assessment can be made granting a statement of the level of trustworthiness of the data protection. There is no way to rule out that you couldn't have guarantees.

How can we protect an algorithm that is sold to a customer with full modification rights?

To protect this algorithm you should preview in the contract a Non-Disclosure Agreement with penalties and indications about the field(s) of business and premises in which the other party is allowed to use the algorithm.

How can we show some code to a customer without fearing that he will copy paste what we did?

NDA or Data prevention loss tools can be used that prevent users to copy algorithms without being aware of that.

Is a contract a copyright work?

Written word is often copyright but laws are in many jurisdictions public domain. In general no but depending on the jurisdiction you could argue for its originality. In practice I would say most lawyers act as if they are not copyrightable, as it oftentimes (esp. for consistency's sake) happens we copy clauses one from the other. For example a contract in a haiku might be original enough. But even then, what the contract defines is not protected – the expression is/can be protected, the underlying facts cannot.

Patents and investments

Could you also expand on copyright registration in China? I recently learnt that this is quite a smart thing to do for software.

The Berne Convention for the Protection of Literary and Artistic Works concluded in Paris in 1971 is an international agreement governing copyright. It is valid in 179 countries, including China.

Are there signs that investment companies (i.e., venture capital) are moving towards the open source licences?

Venture capital in the database sphere in the past few years is heavily investing in the popular open source databases (examples are Mongo DB, Reddis, Elastic). When they want to cash out, i.e., when the open source is popular they change the licence from the open source to something that looks like open source but is not.
At the moment venture capital companies are doing "bait-and-switch" techniques. Major companies are investing into open source and collaborating with others.

In the USA you can patent algorithms and programs; how is it regulated if a piece of code goes to the USA and it is patented?

Such patents should have not been validated at first place if the code was publicly available before, i.e., it is not a new invention. If the code was published before the opened code one can use it if your software operates on their software. If the company still sues you assuming the code was an open source based algorithm that might be addressed to the open network invention definition.

Patents are also territorial. If the registered patent in the USA might not be registered elsewhere. So, as long as you are not breaching the patent in the territory where it is valid that should not be the issue with breaching it.

CONCLUSIONS

Matching the business model with the appropriate IP strategy is key

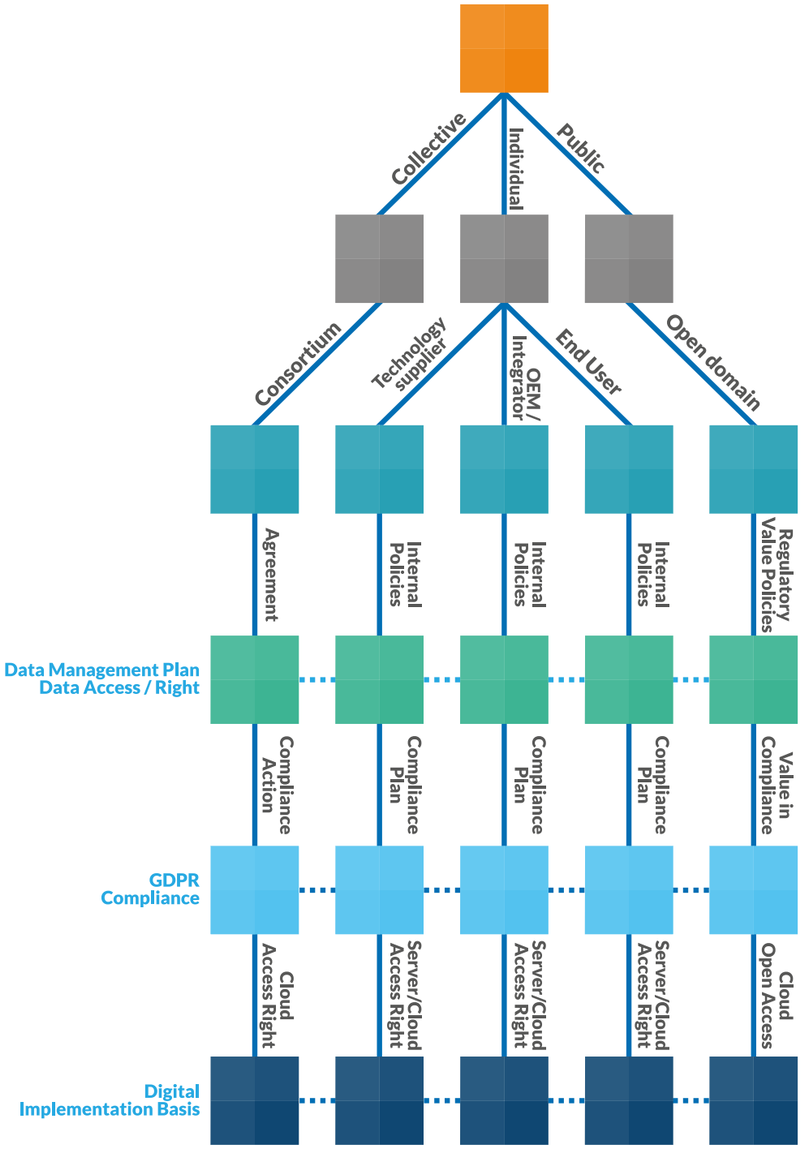
One key overarching recommendation emerged from the workshop discussions, namely to always match a project's IP strategy with the business model of the product or service that is being developed.

Particularly, for data-intensive business models, it is essential that:

- Companies consider and implement data governance strategies that account for the entire data supply chain;
- Companies become aware that simply because certain data are publicly available does not, per se, mean that such data can be used with a blank cheque for any purpose. The terms and conditions of data licences, where specified, must be observed at all times, as well as the principles of data protection law, in so far as processing of personal data is involved;
- Much like with open source software, companies should ensure that the licences of the data they ingest are compatible with the licences under which they intend to release their product. This implies two actions:
- Ensure that the licences of the inbound data are compatible with each other.
- Ensure that there is no conflict between the licences of the inbound data and the licence(s) selected for the outbound product.

The SME experience with data-driven innovation collected during the Go-DIP project has shown that critical issues are identified at the level of data ownership. In a nutshell, the case often arises in which users own their data, but OEMs or integrators, for their part, have an interest in extending their domain of data ownership by combining end user data with their own data. In addition, technology suppliers have a similar interest in also becoming the owner or obtaining access to end users and OEM or integrator data. This generates a complex situation between involved actors and interested parties and potential conflicts in the drafting of contracts.

The decision tree shown in Fig.2 therefore proposes a simple approach based on the lessons learned during the Go-DIP project. It is crucial to define the business case in question at the stage of generating opportunity in the innovation process (see above). The selected branch of the decision tree then defines specific characteristics of data management, GDPR compliance and implementation. Practices are evolving towards a data-based innovation cycle encompassing all innovation actors and end users.



REFERENCES

Further readings:

- Baianat Intellectual Property, The Future of Intellectual Property – Data-driven IP (2021)
- David Lager, Yuejun Sun: The Role of IP in a Data-Driven Business Model (2021)
- Fraunhofer IIS: In the future, successful business models will be built around data (2021)
- Leapyear: Monetizing Sensitive Data (2021)
- WIPO: Intellectual property in a data-driven world (2019)

Sources for choosing the right licence:

https://choosealicense.com/
Dr. Aleš Lipnik, Institute for Economic Research, University of Ljubljana

- [1]Art. 4 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.
- [2]Margoni, Thomas and Kretschmer, Martin, A Deeper Look into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology (July 14, 2021). Available at SSRN: https://ssrn.com/abstract=3886695 or http://dx.doi.org/10.2139/ssrn.3886695, p. 1.
- [3]Deisenroth, M. P.; Faisal, A. A. & Ong, C. S. (2020), Mathematics for Machine Learning, Cambridge University Press, p. 12.
- [4]CJEU, Case C-355/12, Nintendo Co. Ltd, Nintendo of America Inc., Nintendo of Europe GmbH v PC Box Srl, 9Net Srl, 23 January 2014, ECLI:EU:C:2014:25, § 23.
- [5]Art. 7 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.
- [6]Christopher Moran, "Machine Learning, Ethics, and Open Source Licensing (Part II/II)", The Gradient, 2021.
- [7]Art. 6 Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs.
- [8]Copyright registration offices collected from a survey cared by WIPO in 2010
- https://www.wipo.int/copyright/en/registration/replies_survey_copyright_registration.html

APPENDIXES

Appendixes:

- The relevant regulations: In this appendix are reported the relevant EU regulations when coming to Digital IP and future technologies with a short outline on their role and contents.
- Cases of digital IP valorisation: The appendix reports the cases of Digital IP valorisation and exploitation that were collected during the Go-DIP project activities.

Attachments:

- Guide for companies: A ready to use tool for Digital IP management in companies.
- Guide for researchers: A tool dedicated to researchers dealing with Digital IP and supporting them in the exploitation and protection of this IP.

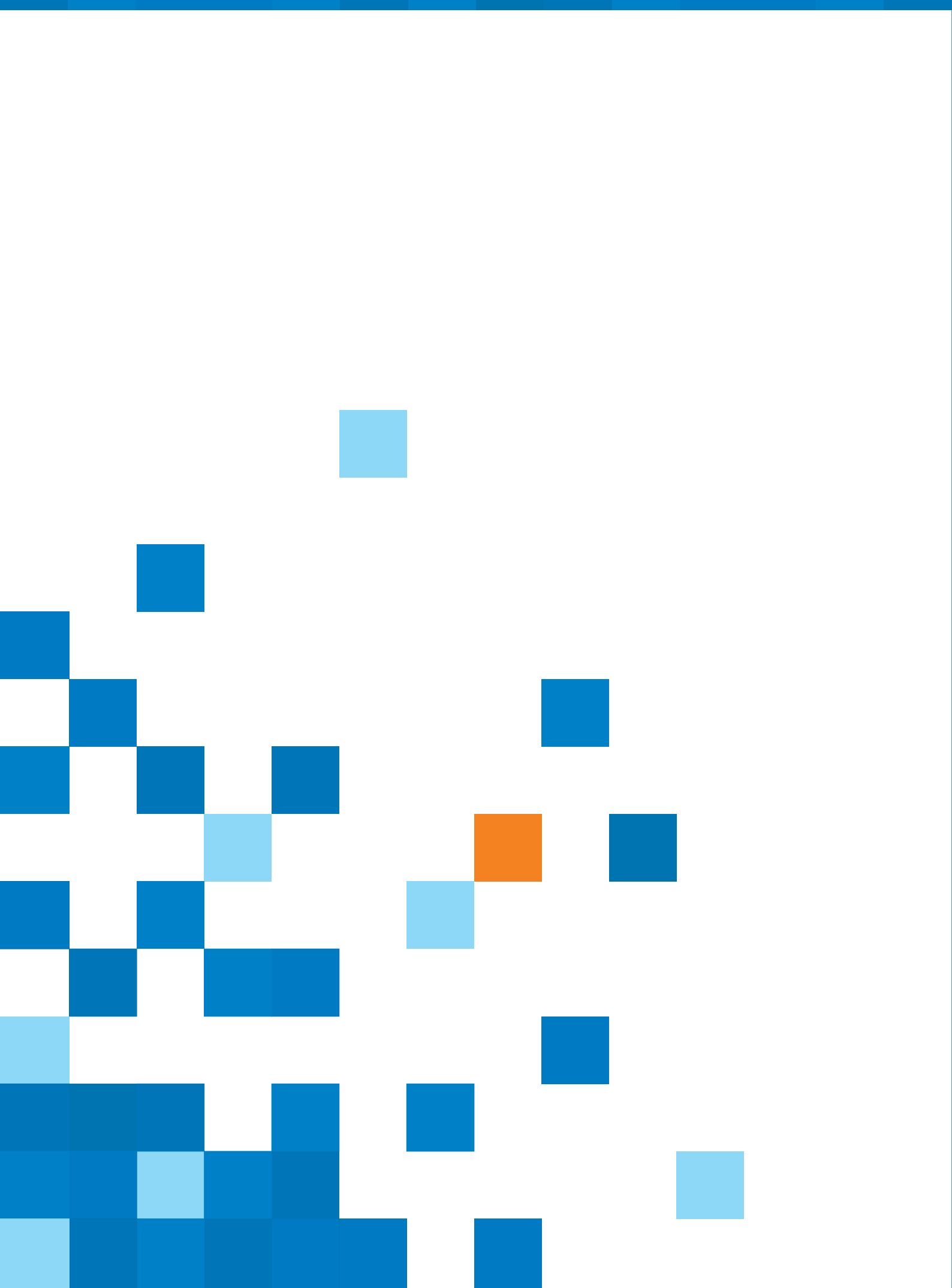
GO-DIP

Design Option Paper

Appendix 1

The Relevant Regulations

Grant Agreement No 970904
Start date of the Project: 1st March 2021
Duration: 12 Months



INDEX

Appendix 1
The Relevant Regulations

A survey performed in the scope of the Go DIP project showed that very few companies were familiar with the European Union's regulations such as Free Flow of non-personal data (FFD) and with the European Data Spaces acts approved by the European Commission in the recent past. More companies were familiar with the Open Data Directive and many more with the General Data Protection Regulation (GDPR) that is applied in day-to-day business practices by European companies in recent years.
Compliance with EU legislation in relation to the digital economy is crucial for businesses. SMEs, therefore, need to better understand the regulatory frameworks that have direct implications for the digital data management in the companies and can have severe implications for companies if they are breaching or infringing the European Union legislation in the various domains of digital data management as presented in this Design Option Paper.
An overview of the legislative background and foreground is provided here in relation to digital data management in companies.

Active Regulations
Open Data Directive

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information

What is it about?

Open Data Directive sets out the rules to allow full exploitation of the potentials of public sector information. It is about a set of minimum rules governing the re-use and the practical arrangements for facilitating the re-use of documents and data held by a public sector bodies such as public libraries, archives, museums, research organisations, including public services that add value for the benefit of re-users, end users and society in general and in many cases for the benefit of the public sector as well. This includes a list of specific high value datasets under each of six themes (Geospatial, Earth observation and environment, Meteorological, Statistics, Companies and company ownership and Mobility).
The Directive also includes data gathered by public services such as water, energy, transport, postal services, public transport services by rail and road, air carriers, or marine transport services which are funded or governed by public bodies. These organisations will retain the discretion to make data available for reuse except where requested in an Implementing Act. Information outside the scope of the public service is excluded.
The Directive introduces an obligation for public bodies to publish available data unless access is restricted or excluded. It brings public organisations under the public service information and it proposes using Implementing Acts to set out lists of high value datasets which must be made available by public bodies for reuse where possible in open and machine readable formats.
This will have particular impact on public bodies who currently charge for their data. Any content regardless of the medium (paper or electronic form, sound, visual or audiovisual recording) or any part of such content must be made available for reuse in open formats, machine readable, via application programmes interfaces – APIs and free of charge unless justifiable.

Implications for companies

More real-time data will be available via APIs for free or at minimal costs. This can allow companies, especially startups, to develop innovative products and services, such as mobility apps. Publicly-funded research data will be made accessible via repositories. Finding, classifying data will be thus made cheaper, easier and faster for reproduction (reuse for services, dissemination, anonymisation, identify necessary protection measures).
From a practical point of view, such data will also bring other benefits to companies such as saving hours finding parking places, quicker response time to save lives, lower traffic costs due to congestion, lower energy bills.

Further information

Data Act: Businesses and citizens in favour of a fair data economy -

INSPIRE Directive

Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007establishing an Infrastructure for Spatial Information in the European Community (INSPIRE)

What is it about?

The Inspire Directive is establishing an infrastructure for use of the spatial information data in Europe, mostly to support Community environmental policies, and policies or activities which may have an impact on the environment. The Inspire Directive addresses the

so-called interoperability of geospatial data sets and services for the exchange of data related to one of the 34 spatial data themes ranging from transportation networks, land use, atmospheric conditions, buildings to habitats and biotopes, oceanographics and population, mining, and protected sites. The Directive addresses need for environmental applications, with key components specified through technical implementation rules. It does so through the creation of the application schemes and geospatial encoding mechanisms (using GML, GeoTIFF and other formats) The INSPIRE Implementing Rules on interoperability of spatial data sets and services (IRs) and Technical Guidelines (Data Specifications) specify common data models, code lists, map layers, and additional metadata on the interoperability to be used when exchanging spatial datasets.

Implications for companies

Through the INSPIRE Directive the European Union has created common standards to facilitate the exchange of information and data between the local, regional, national, and European or international levels and thus support integrated policy decision-making at all levels of government. Originally, the Inspire Directives aim was to make spatial and environmental data available and interoperable to facilitate informed decision-making in policy context. To comply with INSPIRE, organisations needed metadata, harmonised data, and network services. Examples of business data applications provided under the Inspire Directive are monitoring energy performance of buildings, overview of habitats and biotops in tourism monitoring crops and land uses, monitoring traffic and parking areas. Companies can now leverage from the compiled data and by processing digital data they can produce valuable digital data based services and products where data gathered, processed, stored, and used can serve as the "raw" materials to create a new value in the digital economy.

Further information

- Data Specifications | INSPIRE - https://inspire.ec.europa.eu/data-specifications/2892
- Presentation of INSPIRE Directive - https://inspire.ec.europa.eu/conference2021/presentations

General Data protection Regulation (GDPR)

GDPR: General Data Protection Regulation: REGULATION (EU) 2016/679

What is it about?

The General Data Protection Regulation (GDPR) is the privacy and security law passed by the European Union in 2016 that imposes obligations on organisations anywhere, so long as they target or collect data related to people in the European Union. It is designed to give individuals more control over how their data are collected, used, and protected online. It also binds organisations to strict new rules about using and securing the personal data they collect from people, including the mandatory use of technical safeguards like encryption and higher legal thresholds to justify data collection.
The GDPR imposes severe fines against those who violate European privacy and security standards. The GDPR law is a very important one because more and more personal data is entrusted to cloud services and breaches occur daily. The regulation itself is large, far-reaching, and complex, making GDPR compliance complicated, particularly for small and medium-sized enterprises (SMEs).
For example, article 3.1 states that the GDPR applies to organisations that are based in the EU even if the data are being stored or used outside of the EU. Article 3.2 goes even further and applies the law to organisations that are not in the EU if two conditions are met: the organisation offers goods or services to people in the EU, or the organisation monitors their online behaviour.
Key regulatory points of the GDPR are data protection principles and people's privacy rights.

Data protection principles

If you process data, you have to do so according to seven protection and accountability principles outlined in Article 5.1-2:

- **Lawfulness, fairness and transparency** – Processing must be lawful, fair, and transparent to the data subject.
- **Purpose limitation** – You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
- **Data minimization** – You should collect and process only as much data as absolutely necessary for the purposes specified.
- **Accuracy** – You must keep personal data accurate and up to date.
- **Storage limitation** – You may only store personally identifying data for as long as necessary for the specified purpose.
- **Integrity and confidentiality** – Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g., by using encryption).
- **Accountability** – The data controller is responsible for being able to demonstrate GDPR

compliance with all of these principles.

People's privacy rights

You are a data controller and/or a data processor. But as a person who uses the internet, you're also a data subject. The GDPR recognises an extensive list of new privacy rights for data subjects, which aim to give individuals more control over the data they loan to organisations. As an organisation, it's important to understand these rights to ensure you are GDPR compliant.

Data subjects' privacy rights regulated by the GDPR act are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

You can read more on the issues of accountability, data security, data protection by design and by default, when you are allowed to process data, consent to process private information, data protection system's organisation on GDPR.eu website: https://gdpr.eu/

Implications for companies

Companies face severe penalties if they do not comply with the GDPR rules.

Companies need appropriate internal technical organisation and designate data protection responsibilities i.e., appoint a Data Protection Officer (though not all organisations need one) and tasks have to be delegated to a team to:

Maintain detailed documentation of the data you're collecting, how it's used, where it's stored, which employee is responsible for it, etc.

Train your staff and implement technical and organisational security measures.

Have Data Processing Agreement contracts in place with third parties you contract to process data for you.

Other technical measures have to be accepted such as requiring employees to use two-factor authentication on accounts where personal data are stored or to contracting cloud providers that use end-to-end encryption.

Organisational measures are things like staff training, adding a data privacy policy to your employee handbook, or limiting access to personal data to only those employees in your organisation who need it.

If you have a data breach, you have 72 hours to tell the data subjects or face penalties. (This notification requirement may be waived if you use technological safeguards, such as encryption, to render data useless to an attacker).

Other measures companies need to take are:

Data protection by design and by default this means you must consider the data protection principles in the design of any new product or activity. If you think of launching a new application for your company you have to think about what personal data the app could possibly collect from users, then consider ways to minimise the amount of data and how you will secure it with the latest technology.

Design company policy when you're allowed to process data. Don't think about using somebody's personal data for commercial or non-commercial purposes – don't collect it, don't store it, don't sell it to advertisers – unless you can justify doing that with one of the following:

- The data subject gave you specific, unambiguous consent to process the data. (e.g., they've opted in to your marketing email list);
- Processing is necessary to execute or to prepare to enter into a contract to which the data subject is a party. (e.g., You need to do a background check before leasing property to a prospective tenant.)
- You need to process it to comply with a legal obligation of yours. (e.g., You receive an order from the court in your jurisdiction.)
- You need to process the data to save somebody's life.
- Processing is necessary to perform a task in the public interest or to carry out some official function. (e.g., You're a private garbage collection company.)
- You have a legitimate interest to process someone's personal data. This is the most flexible lawful basis, though the "fundamental rights and freedoms of the data subject" always override your interests, especially if it's a child's data.

Consent from a data subject

- Consent must be "freely given, specific, informed, and unambiguous."
- Requests for consent must be "clearly distinguishable from the other matters" and presented in "clear and plain language."
- Data subjects can withdraw previously given

consent whenever they want, and you have to honour their decision. You can't simply change the legal basis of the processing to one of the other justifications.
- Children under 13 can only give consent with permission from their parents.
- You need to keep documentary evidence of consent.

Further information:

https://gdpr.eu/what-is-gdpr/

Free Flow of Data Regulation

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union

What is it about?

Free flow of data regulation is less known than its "twin" the GDPR regulation but can be equally important for businesses using data analytics in their business models (Internet of Things, artificial intelligence and machine learning, etc.). Non-personal data in the framework of this regulation is electronic information that cannot be traced back to an identified or identifiable natural person (or has been anonymised as such). Specific examples of non-personal data include aggregate and anonymised datasets used for big data analytics such as data on precision farming that can help to monitor and optimise the use of pesticides and use of water or data on maintenance needs for industrial machines.
There are two types of obstacles to data mobility that hamper the effective and efficient functioning of data processing and the development of the data economy in general:

- Data localisation requirements imposed by Member States

- Contractual vendor lock-in practices in the private sector, (i.e., situations where customers are dependent on a single (cloud) provider technology and cannot easily switch to a different vendor without substantial costs, legal constraints or technical incompatibilities).

The aim of the Free flow of data regulation is to lift these main obstacles and to boost the data economy through facilitating cross-border exchange of data by enabling companies to store non-personal information anywhere in the EU.
One of the main issues addressed by this regulation are **'data localisation requirements'**, i.e., the obligations imposed by Member States for companies to host data centres in the national territory of a Member State and/or the obligation to process data domestically. These data localisation requirements were stifling the development of the EU Digital Single Market since they obstruct the emergence of data innovation ecosystems across European borders as they require European companies to copy their IT infrastructure in several Member States and this increases the cost for data storage (providers) and decreases potential European wide competition. This regulation now enables Member States banning to impose any requirements to either localise or process data domestically and allowing for the emergence of more efficient and centralised data storage systems (e.g., cloud services, which provide a centralised storage space for large datasets). Regulation also imposes a self-regulation of companies against vendor lock-in i.e., service providers making it more difficult for users to switch to other service providers and leading to a lack of competition between cloud service providers in the European Union and a lack of data mobility.
The Regulation now facilitates and encourages EU companies to develop self-regulatory codes of conduct in order to improve the competitive data economy based on the principles of transparency, interoperability and open standards.

Implications for companies

In practice, the Regulation enables data storage users to transfer their data from one provider to another or back to their on-premise systems in a way that is easy, clear and transparent, by way of codes of conduct. These should be comprehensive and should cover at least the key aspects that are important during the process of transferring data, i.e., (i) the processes used for, and the location of, data back-ups, (ii) the available data formats and support, (iii) the time required prior to initiate the porting process and the time during which the data will remain available for porting, etc.

Further information:

https://europa.eu/youreurope/business/running-business/developing-business/using-storing-transferring-data/index_en.htm

Data Governance Regulation

Regulation of the European Parliament and of the Council on European data governance (Data Governance Act).

What is it about?

While the Data Governance Regulation (DGR) creates the processes and structures to facilitate data, the Data Act described below clarifies who can create value from data and under which conditions. DGR aims to increase trust in sharing personal and non-personal data and lower transaction costs linked to B2B and C2B data-sharing by creating a notification regime for data sharing providers and by making secure processing environments through anonymisation techniques such as differential privacy and creation of synthetic data. These providers will have to comply with a number of requirements, in particular the requirement to remain neutral as regards the data exchanged. They cannot use such data for other purposes. In the case of providers of data-sharing services offering services for natural persons, the additional criterion of assuming fiduciary duties towards the individuals using them will also have to be met. The approach is designed to ensure that data sharing services function in an open and collaborative manner, while empowering natural and legal persons by giving them a better overview of and control over their data. A competent authority designated by the Member States will be responsible for monitoring compliance with the requirements attached to the provision of such services.
A licensing system is set up for "data intermediaries." These are organisations which set up commercial arrangements between data holders and data users, but which do not themselves add extra value to the data. Data intermediaries need to meet licence conditions designed to ensure their independence and restrict their re-use of data and metadata. The requirements will affect those offering data marketplaces and (possibly) consent management platforms. There are additional restrictions applicable to those involved in re-use of public sector data.
Implications for companies

Implications for companies

The regulation makes it easier and cheaper for companies to access and use publicly available data when:

- Public sector data is available for re-use, in situations where such data is subject to rights of others.

- Sharing of data among businesses against remuneration in any form is possible.

- Personal data to be used with the help of a 'personal data-sharing intermediary' is allowed and designed to help individuals exercise their rights under the General Data Protection Regulation (GDPR).
o allowing data use on altruistic grounds is possible;

Further information

https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2103

Data Act

Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)

What is it about?

Data Act – was adopted by the Commission on 23 February 2022. The Data Act complements the Data Governance Regulation proposed in November 2020, the first regulatory framework of the European strategy for data. While the Data Governance Regulation creates the processes and structures to facilitate data, the Data Act clarifies who can create value from data and under which conditions.
The Data Act will ensure fairness by setting up rules regarding the use of data generated by Internet of Things (IoT) devices.
Users of objects or devices generally believe that they should have full rights of the data they generate. However, these rights are often unclear. And, manufacturers do not always design their products in a way that allows users, both professionals and consumers, to take full advantage of the digital data they create when using IoT objects. This leads to a situation where there is no fair distribution of the capacity to build on such important digital data, holding back digitisation and value creation.
Furthermore, the Data Act aims to ensure consistency between data access rights, which are often developed for specific situations and with varying rules and conditions.

Implications for companies

- The Data Act will give both individuals and businesses more control over the data they generate through their use of smart objects, machines and devices, thereby allowing them to enjoy the advantages of the digitisation of products.

- By having access to the relevant data, aftermarket services providers will be able to improve and innovate their services and compete on an equal footing with comparable services offered by manufacturers. Therefore, users of connected products could opt for a cheaper repair and maintenance provider – or maintain and repair it

themselves. This way, they would benefit from lower prices on that market. This could extend the lifespan of connected products, thus contributing to the Green Deal objectives.

- Availability of data about the functioning of industrial equipment will allow for factory shop-floor optimisation: factories, farms, and construction companies will be able to optimise operational cycles, production lines and supply chain management, including based on machine learning.

- EU businesses, especially SMEs, will have more possibilities to compete and innovate on the basis of data they generate thanks to data access and portability rights. It will be easier to transfer data to and between service providers and this will encourage more actors, regardless of their size, to participate in the data economy.

Further information:

https://digital-strategy.ec.europa.eu/en/policies/data-act

Digital Services Act

What is it about?

The Digital Services Act strengthened the mechanisms for the removal of illegal contents and better protected users' fundamental rights online, including the freedom of speech. It also creates a stronger public oversight of online platforms, in particular for platforms that reach more than 10% of the EU's population. The rules better protect consumers and their fundamental rights online and establish a powerful transparency and a clear accountability framework for online platforms.

To better protect European values and users this act introduces and prescribes:

- Measures to counter illegal goods, services or content online, such as a mechanism for users to flag such content and for platforms to cooperate with "trusted flaggers".

- New obligations on traceability of business users in online marketplaces, to help identify sellers of illegal goods.

- Effective safeguards for users, including the possibility to challenge platforms' content moderation decisions.

- Transparency measures for online platforms on a variety of issues, including on the algorithms used for recommendations.

- Obligations for very large platforms to prevent the misuse of their systems by taking risk-based action and by independent audits of their risk management systems.

- Access for researchers to key data of the largest platforms, in order to understand how online risks evolve.

- Oversight structure to address the complexity of the online space: EU countries will have the primary role, supported by a new European Board for Digital Services; for very large platforms, enhanced supervision and enforcement by the Commission.

Implications for companies

Businesses have access to more information on how their products or services are performing on third party platforms
No more unfair ranking of gatekeepers' own services and products compared to those offered by other businesses on the same platform
Businesses are able to more easily attract consumers who can no longer be locked in by gatekeeper platforms
Easier for smaller businesses and new entrants to grow and expand, and compete with gatekeeper platforms.
Increased competition, improved quality of services for end users
Removing disincentives for companies to take voluntary measures to protect their users from illegal content, goods or services
Businesses use new simple and effective mechanisms for flagging illegal content and goods that infringe their rights, including intellectual property rights, or compete on an unfair level.
Businesses may also become 'trusted flaggers' of illegal content or goods, with special priority procedures and tight cooperation with platforms.
Act imposes obligations to different services as described in the following Table 1.

Further information:

The Digital Services Act: ensuring a safe and accountable online environment
https://ec.europa.eu/info/digital-services-act-ensuring-safe-and-accountable-online-environment_en

Table 1: Digital service Act prescribed obligations for service providers.

Obligations	*Intermediary services*	*Hosting services*	*Online platforms*	*Large platforms*
Transparency with reporting	■	■	■	■
Requirements on term of service due to account of fundamental rights	■	■	■	■
Cooperation with national authorities following orders	■	■	■	■
Points of contact and where necessary legal representative	■	■	■	■
Notice and action and obligation to provide information to users		■	■	■
Complaint and redress mechanisms for out of court dispute settlement			■	■
Trusted taggers			■	■
Measures against abusive notices and counternotices			■	■
Vetting credentials of third party suppliers			■	■
User-facing transparency of on line advertisements			■	■
Reporting criminal offences				■
Risk management obligations and compliance officer				■
External risk auditing and public accountability				■
Transparency of recommended systems and users choices for access information				■
Data-sharing with authorities and researchers				■
Codes of conduct				■
Crisis response cooperation				■

Regulations in preparation during 2022

Machinery regulation

Link to Proposal: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0202

What is it about?

The revised Machinery Directive 2006/42/EC is called "New Machinery Regulation," and after a revision in 2021 the existing Machinery Directive from 2006 new regulation got three main additions:
Ensuring the safe use of artificial intelligence systems in machines;
Legally clarify some current provisions and standardise the regulations leaving no room for interpretation;
Allowing and encouraging the use of digital formats for the accompanying documentation of the machine.
This revised Directive is standardising health and safety requirements within the European Union to ensure that they are up to date with technological progress (such as artificial intelligence), the design, construction, and trade of machinery. The old directive did not sufficiently cover the new risks arising from emerging technologies, such as those relating to human-robot interaction or artificial intelligence implications, given the increasing use of collaborative technologies in industry. The complexities of managing increasingly connected machines and software updates after the product have been placed on the market were added as well.

Implications for companies

With a view to digital transformation, the new regulation intends to encourage the use of digitised documents, abandoning paper where possible and thus embracing the increasingly growing sustainability policy advocated by the European Union.
The new Machinery Regulation contains a series of measures to protect the information needed to certify the conformity and traceability of machinery.
For those who do not comply with the standards and procedures of the Regulation, there are sanctions calculated on the basis of the highlighted discrepancies and decided by the Member States.
Manufacturers must always, for each machine, provide a European declaration of conformity, and ensure that all components relating to the machine are clearly and comprehensively identified and traceable in the language of the product's country of destination.
This declaration consists of a series of documents certifying the product against the standards required by the legislation; these standards must be met by the manufacturer, right from the design, and construction phase of the machine.
Handling of the artificial intelligence systems in manufacturing and products are regulated in particular, AI ensuring a safety function, placed independently on the market or a machinery containing AI ensuring a safety function will be considered as a high-risk machinery, and will require a validation by a third party.
This will also impact software ensuring a safety function.

Further readings

https://ec.europa.eu/docsroom/documents?locale=en&keywords=machinery

Digital Market Act

Link to Proposal: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0842&from=en)

What is it about?

Along with the Digital Services Act (DSA), Digital Market Act (DMA) is one of two flagship pieces of EU legislation aimed at regulating larger online platforms.
DMA will address the way some tech companies have exploited their size and entrenched position to become so-called "gatekeepers," whose control over access to digital markets gives them competitive advantage over other companies and consumers.
The Digital Market Act addresses nearly every significant digital service: online marketplaces and app stores, search engines, social networks, video-sharing platforms, operating systems, cloud services, certain interpersonal communications services like WhatsApp calls or web-based email services, and advertising networks affiliated with any of the above, including core platform services: web browsers, virtual assistants (such as Siri or Alexa), and connected TV.

Implications for companies

Negative practices such as ranking services and products offered by the gatekeeper itself higher than similar services or products offered by third parties on the gatekeeper's platform or not giving users the possibility of uninstalling any pre-installed software or app will be limited to advance fair competition.
The rules should boost innovation, growth and

competitiveness and will help smaller companies and start-ups compete with very large players.
Includes additional requirements on the use of data for targeted or micro-targeted advertising and the interoperability of services, e.g., number-independent interpersonal communication services and social network services.
End users will get the option to uninstall pre-installed software applications, such as apps, on a core platform service at any stage.

Further information

https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

European Artificial Intelligence Act (AIA)

Link to Proposal: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

What is it about?

The new AIA assigns applications of AI to three risk categories. First, applications and systems that create an unacceptable risk, such as government-run social scorings are banned. Second, high-risk applications, such as a CV-scanning tool that ranks job applicants, are subject to specific legal requirements. Lastly, applications not explicitly banned or listed as high-risk are largely left unregulated.

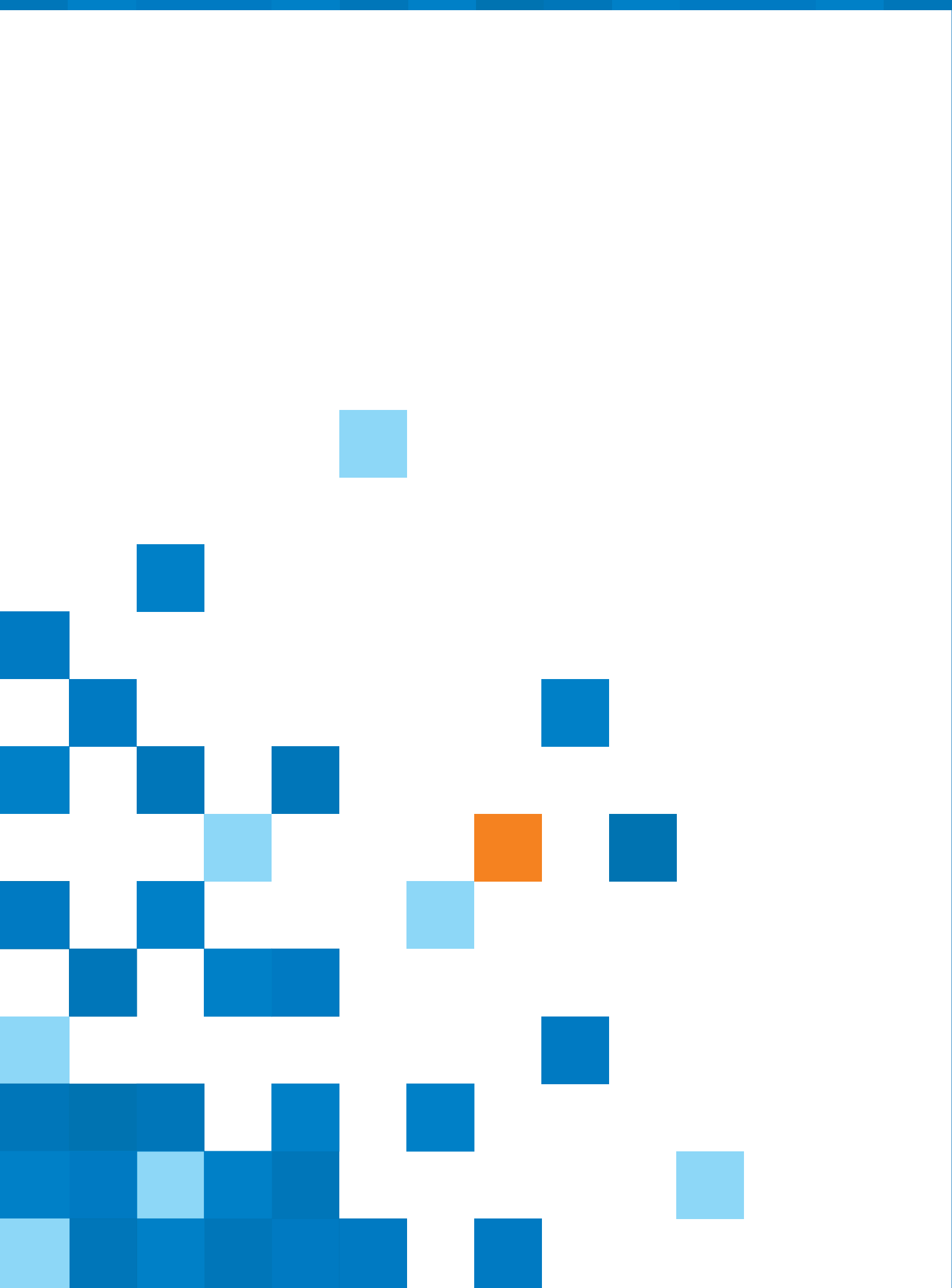
GO-DIP

Design Option Paper

Appendix 2

Cases of digital IP valorisation

Grant Agreement No 970904
Start date of the Project: 1st March 2021
Duration: 12 Months



INDEX

Appendix 2
Cases of digital IP valorisation

Selection of cases

These cases have been selected in the scope of the GO Dip project to give concrete examples of management and valorization of digital IP and data in the three project verticals: legal aspects; Ip agreements; business models.

Parts of the cases have been collected during the three peer learning workshops and local events in 2021 and 2022. The experts group helped us identify cases, with their collection and comments.

Most of the examples come from industry, but we also collected cases from RTO and academia.

Guide for reading

Each case is categorised according to the main topic(s) and specifications.

Main topics:

- Legal aspects of digital IP and data management
- Digital IP and data agreements
- Data driven innovation and business models

Specificities:

- Digital IP – examples software, AI, Machine learning
- Industry process – examples of digital IP and data used in industrial processes
- Product Data – Examples of use of data for product or service customization
- SAAS – Examples of use of software as a service
- Cloud applications - Example of cloud based services
- Open source - Example of FOSS business models
- Artificial Intelligence/Machine Learning
- GDPR - Relevant GDPR compliance aspects

GENEPLANET

Case	Geneplanet is the leading European provider of innovative preventive health solutions based on genetic testing. The company offers whole genome sequencing (WGS) to provide the most accurate information about genetic predispositions as soon as science detects them without further testing.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	☐ Digital IP ☐ Industrial Process ■ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ☐ AI/ML ■ GDPR
Description	**Health Intelligence Platform** This is an interdisciplinary project addressing health challenges and the ICT sector. A personalised platform combines genetic, blood analysis and lifestyle information i.e. predictive diagnostics data. The company has developed through the platform a type of service that has not yet been marketed: it is an innovative global solution based on the symbiosis of high-tech analytical and IoT services. Through integration of analytical data and data from personal wearable sensors, the platform provides the user with user services in the field of diagnostics, on-line monitoring and recommendations for a healthy lifestyle. The company collects bio data through sampling of saliva, (personal kits sold online, followed by DNA extraction and sequencing of genome). Geneplanet collects data in digital form that are proprietary data and can only be used for research if the customer gives written consensus (GDPR). Company has also developed multiple questionnaires to collect personal health data. Once collected data is protected by protocols and only accessible to the authorised personnel within the organisation under strict protocols. Data is packaged and sold to individual customers (buyers of the kits) marketed online. Collected data also enables improvements with predictive modelling. **Example:** customer is diagnosed with a high risk for melanoma cancer. DNA sampling enables a more targeted diagnostics and risk mitigation activities are than prescribed through a products such as healthy diets, fitness programmes and so on.
Impact on company	■ Personal, digitally collected data is used for predictive analytics and modelling to sell targeted therapies & health & wellness products i.e. develop health care products ■ The company cooperates with more than 500 clinics and hospitals around the world, as well as many insurance firms, companies and health and wellness centres.
Comments	Geneplanet has won an award for the best biotech startup in Central and Eastern Europe and was ranked among the 1000 fastest-growing companies in Europe in 2019.

WONDERFLOW

Case	Wonderflow is a fast-growing startup that uses AI-based NLP and predictive technology to extract value from voice of the customer data. They act as data processors for big players such as TomTom, Philips, Colgate.
Main Topic	☐ Legal aspects ■ IP Agreement ■ Business Model
Specificities	☐ Digital IP ☐ Industrial Process ☐ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ■ AI/ML ■ GDPR
Description	**Health Intelligence Platform** Wonderflow unique hybrid approach to text analysis combines an industry-leading team of linguists with top-notch artificial intelligence, resulting in vertical-specific Natural Language Processing engines that will get you an edge on the competition. Their platform provides the clients with the most accurate sentiment analysis on the market for all of your unstructured text, with no configuration required on their side. The data available at the clients premises is managed and exploited by the Wonderflow platform. To do so, relevant personal data are used and elaborated and top-level compliance to the relevant legislation and standards is granted.
Impact on company	■ The capacity in managing agreements with relevant actors and compliance with different international regulations such as GDPR in Europe is a point of strength that is in the company DNA. ■ The company has a data exploitation oriented business model.
Comments	Wonderflow usually includes specific clauses in an agreement for data processor regarding: ■ Own Personnel ■ Appropriate measures for security ■ Subprocessors ■ Handling of data subject rights ■ Data breach ■ Data retention policy ■ Audit rights ■ Data transfer Further information on those specific clauses are reported in the DOP complete document.

AZZURRODIGITALE

Case	AzzurroDigitale is an Italian startup that helps manufacturing companies to join the digital transformation. Cyber Physical systems used by their clients collect data, organize and extract meaningful outcomes based on that data.
Main Topic	■ Legal aspects ☐ IP Agreement ☐ Business Model
Specificities	☐ Digital IP ■ Industrial Process ■ Product Data ☐ SAAS ■ Cloud ☐ Open Source ☐ AI/ML ☐ GDPR
Description	AzzurroDigitale accompanies manufacturing companies in their path of digital transformation in the field of operations. They are specialized in the transformation of factories starting from people and workforce management, and they consider technology as a powerful enabler of change. **Example:** Advanced Workforce Management System (AWMS) is a digital lean solution that, using advanced machine learning-based algorithms, allows factory workers to be scheduled in real time while respecting workers' skills, limitations and restrictions, making the organization more efficient.
Impact on company	■ Important role in the AzzurroDigitale activities is connected with GDPR. In particular the topics that were highlighted is the storage of the data that need to be coherent with the regulation. For example, in orde to guarantee the GDPR compliance their suggestion is to maintain data stored inside Europe. ■ The data driven business model that is core of the AzzurroDigitale activities in relation to the software and digital IP often previews to leverage Freedom to Operate clauses in the agreements in order to relieve client companies from risks connected with due diligence.
Comments	AzzurroDigitale was cited in the Top Manufacturing Startups and Companies in Italy for 2021.

Ecosteer

Case	Ecosteer technology gives consumers ownership rights over their data streams. Individuals should be empowered to be in control of their data through tools and means to decide at a granular level about what is done with their data. In addition, rules for novel data intermediaries could be considered, guaranteeing their role as a neutral broker.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	☐ Digital IP ☐ Industrial Process ☐ Product Data ☐ SAAS ■ Cloud ☐ Open Source ☐ AI/ML ■ GDPR
Description	The company provides a decentralised data backend with intrinsic security supported by encoded communication that wants to interpose personal data companies and persons sharing those data in a new way. People in this approach are informed of the type of data sharing process, choose which data cloud be shared and which not and get rewarded based on the number of companies accessing their data. The business model is related to sharing of personal data in a new way, going beyond GDPR and sharing revenues with the data owners.
Impact on company	■ The dataset is managed on a cyber secure basis and data is not delivered as a full package including information not needed to the specific client. The trust between personal data sharers and the company is also guaranteed by the anonymization of the data directly by the data processor. The client company willing to access that data could be incentivized on one hand to require only necessary data, on the other hand to consider the data processor company as a better alternative partner for the sustainable business model implemented. ■ From their website: By giving consumers exclusive control over third-party access to their data, EcoSteer Data Ownership Platform enables brands to establish a direct relationship with consumers and access their data in a manner that is informed and transparent, leading to a new One-2-One mass marketing model.
Comments	Geneplanet has won an award for the best biotech startup in Central and Eastern Europe and was ranked among the 1000 fastest-growing companies in Europe in 2019.

Financed Project Consortium Agreements

Case	The project on European mobility and the coordinator gained a stronger reputation as leader of such large-scale collaborative cross-border validation activities on cooperative, connected and automated mobility.
Main Topic	■ Legal aspects ■ IP Agreement ☐ Business Model
Specificities	■ Digital IP ☐ Industrial Process ☐ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ☐ AI/ML ☐ GDPR
Description	The case study represents the complex settlement of opposite interests between the parties of an H2020 project consortium agreement on ICT and telecommunication, notably affecting the exploitation of the project results in terms of IP. The consortium was composed of big manufacturing industries, technology development enterprises, research centres, universities and SMEs. A first discussion pòoint regarded a big industry which was forcing the consortium to a free-royalty IP regime thus raising concern and objections from the research providers. A second point was related to a struggle between a big enterprise and a corporate developer concerning the mutual transfer of IP rights over their jointly owned results in case of patent filing on a certain territory by one of the two.
Impact on organisation	■ Commercial exploitation of jointly owned digital IP is an issue which may raise very sensitive interests. They came to consider and understand that exploitation by the party itself can be allowed while third party licensing has to undergo a further business agreement between the joint IP owners. In the case of Open Source, no joint Results would have become subject to an OS licence unless the respective joint owners had agreed to this. ■ Regarding the patenting issue, other specific clauses were drawn. Only the joint owner who would have elected to file for and/or maintain a patent application in a particular country had full control over its preparation, prosecution, maintenance and IPRs enforcement in that particular country, while being liable for all costs related to the filing and/or maintenance of the patent. "Full control" is the keyword here. ■ In order to allow a big corporate developer to sign the agreement they had to establish a specific "ad personam" exception, which is not usual at all. In case, as a joint owner, such party would not agree on the filing of a patent concerning such joint result in a particular country, such party would not be constrained to transfer its part of the joint result to the other joint owner. Meaning, no "full control" allowed to the patenting party without such specific non-patenting (and non-paying) party consent.
Comments	Geneplanet has won an award for the best biotech startup in Central and Eastern Europe and was ranked among the 1000 fastest-growing companies in Europe in 2019.

Original+

Case	From their website: Whether you are an ambitious first-line rider or a chilled skier seeking a comfortable ride: With custom skis from ORIGINAL+ you can carve your own lines into the snow. Produced in Austria exclusively for you and yet affordable. For your plus in individuality and more fun riding.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	■ Digital IP ☐ Industrial Process ■ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ☐ AI/ML ☐ GDPR
Description	Original+ is a startup from Salzburg in the ski sector. The company is not a traditional ski manufacturer, they exploit digitalisation by providing a custom product to the customers. From their website the company guides the end users to define the product explotiting a combination of AI and hardware to identify the best configuration. ■ They configure their ski and customise features for the clients. The company developed a complete IP portfolio in order to preserve their competitiveness and market. ■ They own the copyright on their AI based software ■ They use the data side to customise the ski configuration for the clients ■ They registered a patent on the technical design, ■ They registered a trademark and a special design.
Impact on company	The IP portfolio created from the digital aspects to the more traditional ones has empowered the company and supported the business in an effective way.
Comments	The IP portfolio enabling the business model of Original+ is a balance of aspects protected covering completely the possible points and this makes of them a model company. Particularity of their business model is related to the online only sales supported by AI and data that enables product customisation per each client.

Hyeronimus

Case	Hieronymus creates an inspirational, sensuous space for personal moments. Our roots lie in letterpress printing – a business which demands experience, skill and time. This dedication to craftsmanship is at the heart of everything we do. As a Swiss custom manufacturing atelier, we design, develop and create products of contemporary beauty, from hand-bound notebooks to personal stationery through to writing instruments – for those of us who yearn for elegance and poetry.
Main Topic	■ Legal aspects ☐ IP Agreement ☐ Business Model
Specificities	■ Digital IP ☐ Industrial Process ☐ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ☐ AI/ML ☐ GDPR
Description	For their legal consultancy the company exploited translation services by lawyers for lawyers expert, in legal and financial translation. Translation of contracts has a fundamental role in contract enforcement. Services exploiting neural machine learning translation have been developed and are present on market. One example supporting the translation to swiss legal language is LEx-Machina. The company obtained a certification for confidentiality by ISO.
Impact on organisation	■ Certification for the confidentiality enabled the trust towards their clients and contractors.

ROOMZ

Case	From their website: ROOMZ is the most straightforward and easiest-to-deploy solution to support and create the agile work environments of the future. Right after installation, ROOMZ products will help you to maximize the usage of your hybrid workspaces, while increasing work efficiency and collaboration.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	☐ Digital IP ☐ Industrial Process ☐ Product Data ■ SAAS ■ Cloud ☐ Open Source ☐ AI/ML ■ GDPR
Description	The company developed a SaaS business model related to optimise the use of shared spaces, meeting room display, IoT sensors. human resources, with a facility manager interface. The product combines then hardware and software in a scalable composition for the hardware side. Relevant aspects that were addressed in the company presentation during the second workshop are related to cybersecurity and privacy protection.
Comments	Cybersecurity and privacy protection are relevant aspects for all the companies managing data from third parties. More information on the data management clauses related to those two aspects and contracts are described in the DOP document.

Swiss-SDI

Case	Swiss Statistical Design & Innovation is the specialist in data analysis, both in strategic and analytical consulting and in the development of tools for decision support and data interpretation, in fields as varied as predictive maintenance, energy, human resources, quality control or sales and price prediction.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	☐ Digital IP ■ Industrial Process ■ Product Data ☐ SAAS ■ Cloud ☐ Open Source ■ AI/ML ☐ GDPR
Description	The company is involved in services of data science, the sectors they operate in are energy management, public transports, watch manufacturing industry, car manufacturers. They provide AI services aiming in “enhance human capability“ with strategic consulting, analytics, data interpretation, decision algorithms, commercialization of reports, dashboards creations, prediction as a service and AI algorithms.
Impact on organisation	■ The company protects the software developed with copyright and maintain the source code closed.
Comments	The business model of the company exploits data to train AI for their customers and supports them in the data exploitation. The business model is an hybrid business model between data and software. The protection of their digital IP is achieved by applying the trade secret.

Hiring an expert

Case	Subcontracting of third party developers in order to develope a patent idea in order to reach the market. Key point of this case is related to the copyright management agreement that needed to transfer the copyright on the product to the patent owner.
Main Topic	☐ Legal aspects ■ IP Agreement ☐ Business Model
Specificities	■ Digital IP ☐ Industrial Process ☐ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ☐ AI/ML ☐ GDPR
Description	Hiring a software company to produce software 'for hire' for a project managed by University P.I so that all intellectual rights and I.P are kept in the University. Research institute, a public university, received a grant from private entity to develop technology related to an invention we patented, with view towards producing additional patents. To prove viability, we needed to develop different types of software and make sure the companies that produced the software do not have any intellectual claim to it. The ability to obtain software 'for-hire' in Italy was necessary for further development of I.P within the university.
Comments	Involving 3rd parties in developing software requires substantial preparation and prior consultation with lawyer.

British horseracing board

Case	The British horseracing board produced a database on horse races across England. Those data was exploited by William Hill, an online bookmaker to analyse the history of the races in order to have better prediction of the future events.
Main Topic	■ Legal aspects ☐ IP Agreement ☐ Business Model
Specificities	■ Digital IP ☐ Industrial Process ☐ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ☐ AI/ML ☐ GDPR
Description	The British horseracing board took the William Hill company to court because they appropriated of the data that was collected in years of races. On this aspect the sui generis right's law is the reference protecting the database creators and the IP behind a database.
Impact on organisation	■ Only if it can be demonstrated that a significant investment was made to create a database the sui generis right can be empowered. The significanty investment also correlate with the size of the company. In fact, organisations that have high turnovers will need to demonstrate an effort higher than small organisations with small turnover. The effort is not proportionate to the use or value of the data itself.
Comments	Sui generis rights is the only right that can be valorized on data but needs an effort in tracking all the investment behind the creation. Databases structures can be instead protected by copyright but only if their structure has creative aspects.

RESULT

Case	Result is an SME assisting large scale companies, global corporations and leasing companies. Personal data handling is at the core of the Resulta business.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	☐ Digital IP ☐ Industrial Process ☐ Product Data ☐ SAAS ■ Cloud ☐ Open Source ☐ AI/ML ■ GDPR
Description	The client from a car rental company wanted to increase automation and minimise operational errors and costs. Without current and valid data leasing contracts can not be issued. Rules set by corporations impact employees purchasing powers and limit selection of vehicles. User data along with rules set by corporations and leasing companies own policy for minimal/maximal value of vehicle had to be respected. Based on these parameters the most suitable leasing option is calculated and offered to the customer. Leasing company has a portal where employees of the corporation order their cars which are then subject to a leasing contract. The system Resulta developed enables the user process from checking eligibility to create leasing offer life cycle. The digital data based system handles individual contracts and cooperative contracts. Regular data synchronisation exchanges are organised by both parties. Data is transferred through secured connections via dedicated machines which IP addresses are whitelisted and to mutually authenticate themselves by RCA keys. Personal data is sent by the corporation with SOP or HTTPS request and it is then funnelled into a dedicated database that is encrypted and stored and strictly limited to a handful of employees and data administrators and can be accessed only via special microservice. Because leasing values are calculated by corporation to the salaries of employees the leasing company needs to provide monthly reports. Same applies for the outgoing data. Personal data information is encrypted for processing purposes and then forgotten. It is important that this data is not logged anywhere on the machines where this data was running or any other systems. GDPR is a problem for development as all data handling has to be taken good care of. Company makes sure all data is anonymized before transferring it out of the production environment in case GDPR data use is unavoidable. Consultation with the GDPR officer is needed on that as all steps of deleting traces of use of data have to be followed for mitigating any incidents.
Comments	Security: ■ Business must define clear goals in collaboration with the IT department ■ Integration between large entities can be long drawn process and needs to be planned meticulously ■ A very robust testing regime must be agreed by both parties ■ Documentation must be clear and concise ■ NDAs need to be fully enforced Access: ■ The “need-to-know” policy does not hinder business operations as long as the data can be uniquely identified by other means, rather than by personal information. GDPR: ■ It is important to have a clear picture what and where GDPR data is ■ Having it centralised makes the audits and deletions much easier ■ Encrypted data adds another layer to privacy

Salesqueeze d.o.o.

Case	SaleSqueze is a start up company automating the sales and ordering process in manufacturing industry by providing an AI and ML based online ordering platform for configurable products (i.e. products with multiple parts such as cars, furniture, sewage systems or a simple product such as filter with six configurable properties and 109.350 possible variations) as their business model.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	☐ Digital IP ☐ Industrial Process ☐ Product Data ■ SAAS ☐ Cloud ☐ Open Source ■ AI/ML ☐ GDPR
Description	Such multi components products are hard to understand and order and they are usually ordered using the Bill of Materials list (BOM). Platform provided by salesqueze addresses challenges: How to know which one of thousands components in the configurable product are ready to move forward to close the deal? How to plan sales without historical data from buyers? How to plan supply and know what to keep on stock & when? Through building a digital data based business model company is facing multiple challenges with digital IP exploitation, industry processes, product data collection and processing, artificial intelligence data processing and building a robust business model as SaaS. The platform shows scores and prioritises deals (i.e. tracks behaviour of customers to score deals and calculate priorities for sales team). It forecasts sales (Give B2B/B2C buyers tools to quote and order by themselves and see your live sales pipeline). It optimises supply material flow by analysing orders from BOM lists to detect deprecated options and addons and optimise them. In this way the company on one hand captures buyer's behaviour when buying configurable products and uses AI and ML to make predictions on sales, hot deals and material flows (see what sells to optimise production and supply). A deal scoring and probability engine called Filtrato thus helps customers quickly find potential quotes where customers are ready to close the deal, based on their activity. Company also builds a system that allows manufacturers to include their global B2B network in the online ordering process of their configurable products. By doing this, data is collected about what product variations are being sold, more importantly what BOM lists are ordered, and how much potential sales volume is present on the market.
Impact on organisation	Platform enables development of a new business model developed around AI and ML based services to the manufacturing industry. Solution also plays a crucial role in attracting investments and larger enterprise clients that struggle with accurate forecasting as manufacturers can finally predict their future sales on accurate data and based on BOM analysis and sales data they can forecast materials flow and supply. Impact on other companies/industry ■ Better customer experience for more loyal customers ■ 10x team productivity with digitization and automation ■ Massive margin improvement opportunity ■ Capture new revenue opportunities ■ Engaged and inspired employees Detecting drops and spikes of demand is monitored to have faster response as the lesson on global market purchasing during Covid 19 period in 2021theached, where the productive capacity of many companies around the world suffered. With the material flow they try to find out what sells and what not.

Comments	Company is currently raising a seed investment to develop the solution further and bring this solution to the market. Long term vision is to produce the AI solution for forecasting and bill of materials (BOM) optimization.

IoT based innovation on products

Case	The company commercialised a product with IoT functionalities able to monitor the functioning from remote both for the end user and for the company itself. This enables the monitoring of the functionality and work conditions for the product manufacturer. Because of that the end user needs to accept an agreement for the data that is shared with the manufacturer, moreover this data is used for the maintenance services that are executed by third parties companies. The agreement needed to consider the aspects relative to GDPR.
Main Topic	■ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	☐ Digital IP ☐ Industrial Process ■ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ■ AI/ML ■ GDPR
Description	The company is involved in services of data science, the sectors they operate in are energy management, public transports, watch manufacturing industry, car manufacturers. They provide AI services aiming in "enhance human capability" with strategic consulting, analytics, data interpretation, decision algorithms, commercialization of reports, dashboards creations, prediction as a service and AI algorithms.
Impact on organisation	■ The company is empowered by having access to data useful for product design objectives and to improve the product quality. ■ Moreover, the company differentiated from the competitors and addressed the market with a new solution and new services for their clients.
Comments	GDPR compliance considering third party organisations that will need to use the data collected to guarantee the service was an urgent matter for this business case.

Domel d.o.o

Case	Domel is a development leader in the vacuum motor market. Company creates motion in professional and home appliances, such as floorcare tools, gardening equipment and power tools, in HVAC, in mobility, in industrial applications, in medicine and healthcare and in alternative energy sectors. It is the global leader in the vacuum motor market.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	☐ Digital IP ☐ Industrial Process ■ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ☐ AI/ML ☐ GDPR
Description	Case presented deals with R&D and safety of the brushless electric blowers. Each product is checked for safety, tested, and controlled. Each step is performed on its own machine and the results are migrated to the database. The purpose is to ensure 100% control, to distribute safe products and to ensure that the product meets the buyers' standards. First the motor is checked for electric safety. After that it goes through run in, and the last step is final control. During this process a lot of data is generated such as data on electric safety (testing that no current flows from one point to another point) , on performance (running & testing the power of the electric products for example air blowers) quality control data, measuring electrical parameters (voltage, current and power, speed and vibration at different control voltages, vacuum values and detect possible mechanical faults. Other tests performed by Domel include electric safety for workers and end users, measuring resistance, proper insulation of the blower and compliancy checks (making sure no current flows from one point to the other) and the "run in" tests in a soundproof room. Data on speed and vibration as well as on mechanical faults are also gathered. In all these testing software records data collected about each electric product and a report is prepared on each measured parameter of electric appliances. The blower without defects is visually inspected and transported to packaging. ■ Implication of digitised data on business: Data obtained from testing is used in packaging the products. Each serial barcode is scanned, and the interface returns the data of performed tests. All the data is drawn from the server and we can check when each test was performed. The interface gives us back the time and result of an electrical safety test, run in status and final control status. If the blower skipped a certain operation or it didn't pass it successfully, a red warning lights up. If every motor succeeded the performed tests, the pallet can be finished and sent to the warehouse for shipment. If one (or more) of the three lights are red, the product won't be counted into the sum of the pallets (for example 99/100 of the batch) and the pallet batch cannot be completed. ■ Digital data value added: A client inquires about data that didn't matter to them until present. We can offer that valuable information not only from the present production, but also from the already manufactured batches from years ago. System is designed in a way that is prepared for various customer requirements. If a customer wants an additional parameter checked we just implement the measuring device into the final control system.

Impact on organisation	■ Data enables Domel to meet high demands on the market and gives other companies a competitive advantage as Domel provides value for the end customers in terms of safety, quality, delivery, guarantees and after sales services. Collecting and managing data on each product in the production process gives a very high value added to the company and possibility to sell not only products but also quality services to the end customers. That enables Domel competitive advantage on global markets but also development of its own products and services based on data.
Comments	Domel process is flexible and enables the company to quickly offer to customers free data on their products. Data is valuable for the company and the customers and suppliers both for the present and future applications and use. There will always be an abundance of data. What is important is the potential to select appropriate data in this abundance to advance business. Be aware of your data and its potential uses (current and future users).

Research to business

Case	This case regards a traditional Technology Transfer agreement from a research centre to a company.
Main Topic	■ Legal aspects ☐ IP Agreement ☐ Business Model
Specificities	■ Digital IP ☐ Industrial Process ☐ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ☐ AI/ML ☐ GDPR
Description	The research institute developed a tracking system to cope with Covid19 pandemy. This system is composed of hardware and software linked together. An external company (A) acquired the solution with a subcontracting agreement for an initial number of prototypes and an agreement for a number of systems yearly provision. To guarantee the provisioning of the parts to the subcontractor, the research institute supported the creation of a private company (B) in charge of manufacturing the hardware. To do that the IP necessary was licenced to the new private company (B) enabling it to support the external company with the parts production. Meanwhile the research institute continued to develop the software part. To manage this the agreement previewed a specific improvements clause dedicated to upgrade and enhance the product performances.
Impact on organisation	Company could be licenced for the prototype development and will have a Tier 1 private partner that will be able to maintain the production requests.
Comments	Complex scenarios in Technology Transfer agreements require attention and a view on the IP ownership and due diligence.

Avtolog

Case	Avtolog collects and displays vehicle data under the auspices of the Automotive Association of Slovenia (AMZS). The app shows various data about the car, its owners/users, technical specifications, history based on the car's identification number.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	☐ Digital IP ☐ Industrial Process ☐ Product Data ☐ SAAS ■ Cloud ☐ Open Source ☐ AI/ML ■ GDPR
Description	In addition to the revamped image and mobile app, you can now park your vehicles or the ones you want to store in "My Garage". This will allow you to access them quickly later and without re-scanning the VIN number. By clicking on "Create contract" you can now prepare and print a sales contract for the selected vehicle in three steps.
Impact on organisation	Autolog is an indispensable tool that allows visitors (car owners, buyers, sellers, services) to view available data on the history of the vehicle and helps create a safe and orderly car market. The autologist became part of the AMZS group in October 2019. With its knowledge and experience, AMZS will enable further development of the project. Together, they will continue the mission of the project and continue to strive to make the data publicly available and to create a safe and orderly car market together.
Comments	Companies servicing, selling or renting cars and/or individual owners, buyers and sellers can have a transparent view on the car's conditions and history based on open data.

Tocen.si

Case	Tocen.si is a mobile application using open data that enables the user to easily and uniformly use personal and sustainable forms of mobility.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	☐ Digital IP ☐ Industrial Process ☐ Product Data ■ SAAS ■ Cloud ☐ Open Source ☐ AI/ML ☐ GDPR
Description	You can check the current timetables and occupancy of buses, availability of the Bicikelj city rental bicycles across the city and Avant2GO electric vehicles available in Ljubljana and its surroundings in one place. If you are travelling to the city by car, you can easily check the current occupancy of parking lots and garages in the city. With the Tocen.si application, travelling around Ljubljana is quick and easy and more sustainable. Visitors save time, can make informed choices on where to park, on availability of rental cars or bicycles or using public buses as means of transportation in and around the city.
Impact on organisation	Companies save time by finding parking and the best transportation system in and around the city. Car sharing and rental companies and bicycle rental services enable bigger use of public transportation, reducing pollution and traffic in the city, replacing it with more sustainable means of travelling.
Comments	Not produced by a private company. Publicly managed application. Free and open data is used to the benefit of citizens and visitors.

Covid-19 Sledilnik

Case	The "Covid-19 Tracker Slovenia" is a crowdsourcing project that collects, analyses and publishes data on the spread of the SARS-CoV-2 coronavirus, the cause of COVID-19, in Slovenia.
Main Topic	■ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	☐ Digital IP ☐ Industrial Process ☐ Product Data ☐ SAAS ☐ Cloud ■ Open Source ☐ AI/ML ☐ GDPR
Description	Public gets a better overview of the magnitude of the issue and a proper assessment of the risk. It collects data: the number of tests performed and the number of confirmed infections number of confirmed infected by categories: by age, sex, regions and municipalities records of hospital care of patients with COVID-19: hospitalised, in intensive care unit, critical condition, discharged from hospital care, recovered monitoring of individual cases, especially in critical activities: health care workers, nursing homes, civil protection capacity of the health system: number of beds, intensive care units, respirators for breathing etc. COVID-19 Sledilnik is an open source project that would not be possible without the hard work of the community members as well as numerous suggestions, comments and contributions from other people.
Impact on organisation	All data gathered can be downloaded and shared in the CSV databases, REST API and Google docs tables. Different charts (on demographics, on daily occurrences, regional distribution etc.) are available for downloads and reuse by media, individuals and companies for daily use.
Comments	It is a community project.

4MINES

Case	4MINES is offering an innovative integrated system consisting on a platform that combines cloud, edge to collect, process and report data about the safety devices of mining machinery and includes a tool-kit to be used by supervisors and technician during the inspection phases to identify most critical elements to be inspected and to report results of on-field verifications.
Main Topic	☐ Legal aspects ■ IP Agreement ■ Business Model
Specificities	☐ Digital IP ☐ Industrial Process ☐ Product Data ☐ SAAS ■ Cloud ☐ Open Source ■ AI/ML ☐ GDPR
Description	4MINES is a centre of the Technical University of Madrid (UPM) created to bring on the market results of an EIT Raw Material Projects called SAFEME-4MINE. 4MINES has been created by the coordinator of SAFEME4MINE project, LOM, which is a centre of UPM too. An IP Agreement between all consortium partners has been stipulated that states that the partner generating any Intellectual Property it also owns it. LOM had the background of the SAFEME4MINE project and developed the foreground that was needed in order to commercialise the project. LOM's background and foreground was licensed for free to 4MINES for commercial purposes. Another partner, FBK, has developed the foreground during the SAFEME-4MINE project, a software (close source), needed for the exploitation of the product. A licence agreement has been stipulated between FBK and 4MINES to allow the use of the software for free for a specific amount of time, 5 years, for commercialising purposes. 4MINES will pay royalties, different each year, based on the net income generated by the commercialization. The contract between 4MINES and FBK does not include the maintenance of the software. 4MINES has to define a new contract in order to maintain the software generated by FBK.
Impact on organisation	4mines solution is based on the worker integrity and it is, although affecting the production and the efficiency. Instead other maintenance machinery solutions on the market consider only the functional conditions of the machinery, and they do not take into account employee safety.
Comments	In the licence agreement between FBK and 4MINES it could have been agreed on a fee for the maintenance of the software in order to guarantee immediately the maintenance of the software. Another option could be to do a contract with a software house. The latter company has to work on the software created by a third party which sometimes can be difficult.

Ultra AI

Case	Ultra AI provides a system that allows the diagnosis of viruses without the use of magnetic resonance imaging.
Main Topic	☐ Legal aspects ■ IP Agreement ☐ Business Model
Specificities	■ Digital IP ☐ Industrial Process ☐ Product Data ☐ SAAS ☐ Cloud ■ Open Source ☐ AI/ML ☐ GDPR
Description	The system uses ultrasounds that allow staff to monitor the lung situation without incurring the contraindications of magnetic resonance imaging. In addition, the developed system allows the doctor to monitor the situation remotely without moving the patient from his room. This is particularly advantageous when the patient is potentially contagious. The scientific validity of the techniques has been validated during the coronavirus pandemic. The software was developed by researchers of the University of Trento using open source licences. During the pandemic, researchers worked in collaboration with healthcare professionals and understood the effectiveness of the software solution. Two serial entrepreneurs got in contact with the professor because they were interested in creating a new business based on the developed software and they wanted to support drafting the Go-To-Market strategy. The University of Trento in collaboration with the two serial entrepreneurs applied and won an EIT Digital call supporting the exploitation of innovative digital solutions. Meanwhile, Ultra AI startup company has been constituted in order to commercialise the software. Since some of the digital assets used by Ultra AI company were owned by the University of Trento, a know-how agreement was stipulated between Ultra AI and the University.
Impact on organisation	The startup offer a solution with the following characteristics: absence of ionising radiation (particularly relevant for pregnant women and children), non invasive, Real Time results, delocalized data acquisition, pre-diagnosis readiness, easy to use, low cost of the instrumentations and their management.
Comments	Open licences used for the developed software had several implications on the startup business model.

Security embedded

Case	Security embedded is a software-based Trusted Execution Environment for low-powered and resource-constrained embedded systems. It is a secure software layer that can be installed on many low-end IoT devices, allowing other applications installed on the devices to run safely and free of malware. It does not rely on expensive hardware and can be installed from remote, thus allowing its fast and cheap deployment on all the legacy and low-cost devices.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	☐ Digital IP ☐ Industrial Process ☐ Product Data ■ SAAS ■ Cloud ☐ Open Source ☐ AI/ML ☐ GDPR
Description	Security embedded is a startup company constituted to commercialise the results generated within a EIT Digital project called MCU Fortifier by a partner, University of Trento . During the MCU Fortifier an IP Agreement between all consortium partners has been stipulated that states that the partner generating any Intellectual Property it also owns it. University of Trento had a strong background and a foreground (Digital IP) that could have been used for a business creation. The professor involved in the project and a group of PHDs have decided to pursue a startup creation constituting the Security embedded. The professor will be just a technical advisor while the PhD have become employees of the startup company. The startup, in order to commercialise and implement project results, made a licence agreement with the university of Trento in order to use the source code exclusively. An amount has been paid to the university (lump sum) and it has been agreed to provide royalties (different each year) on the net income of the startup and/or investments.
Impact on organisation	Cybersecurity is a challenge for many companies and institutions. Security embedded offers a trusted solution able to counter the problem.
Comments	The professor involved in the project is a technical advisor while the PhD have become employees of the startup company. A maintenance fee was not contemplated in the licence agreement between the University of Trento and the startup company because the software was developed by the people that are now working in the startup company. Hence, the startup will directly maintain the software. Since the software was owned by the university, the startup had to send an official request to start the negotiation to get the licence.

Sibylla

Case	Sibylla has developed a patent-based software platform to apply innovative algorithms and drug design protocols derived from advanced mathematical methods of theoretical physics. Sibylla's platform enables to reveal with atomic resolution the folding and misfolding mechanisms of bio-medically relevant proteins, thereby unveiling an entirely new class of pharmacological targets.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	■ Digital IP ☐ Industrial Process ☐ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ☐ AI/ML ☐ GDPR
Description	Sibylla was born out of a scientific challenge, the PPI-FIT protocol (Pharmacological Protein Inactivation by Folding Intermediates Targeting). A patent was filed by three different entities: University of Trento, Telethon and Istituto Nazionale Fisica Nucleare (IFNN) that owned the patent in different percentages. IFNN owned half of the patent and therefore it was chosen as the main entity in charge of the technology transfer activities. Some researchers of the team of the three entities have divided to constitute a spin-off company in order to bring the technology on the market and they constitute Sibylla. A negotiation between the Sibylla and the IFNN in order to get the licence of the technology has immediately started. Meanwhile Sibylla started looking for investments in order to boost the implementation of the technology. Finally, a licence agreement between the three entities and Sibylla has been signed. An upfront fee was paid immediately while the whole amount of money has been paid in a different manner. Moreover, Sibylla committed to pay royalties on future net income and investments received. Additionally Sybilla raised a series A round.
Impact on organisation	Sibylla's mission is to unveil a novel class of therapeutic targets allowing the treatment of currently incurable diseases and offering best-in-class therapies.
Comments	Sybilla raised the investment immediately after the signing of the licence agreement with the three entities. Sibylla bases its business on the patent which is part of the value of the spinoff company. Hence, the investor would not have invested in the spinoff company without it. Moreover, since the patent was owned by public institutions, Sybilla has to send an official request to start the negotiation to get the licence of the patent.

Semiconductor startup

Case	The company is a disruptive semiconductor start-up. Their goal is to deliver a new category of optical sensors to give machines the eyes they need to intelligently see, map and sense the world in the safest and most efficient way. Technology companies have been working for decades to deliver 3D depth perception systems for machines to understand, process and autonomously make decisions. We aim to outperform competition such as LiDAR, ToF and Dynamic Vision and Event Sensors by a factor 100x in areas such as detection speed, power consumption, processing requirements and scalable (super)resolutions.
Main Topic	■ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	■ Digital IP ☐ Industrial Process ☐ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ■ AI/ML ☐ GDPR
Description	The company was looking to integrate new technologies to enhance its services capacity. The company has contacted an Italian research centre called Fondazione Bruno Kessler (FBK) to leverage on their know-how and their patented technology to boost their business. Firstly, the company wanted to test the patented technology in order to validate if it was what they were looking for. An option agreement was stipulated between the company and FBK to allow the company to use the technology exclusively for an amount of time (around 6 months) and stating that the company has the priority to acquire or licence the patented technology. After the option period, the company agreed with FBK to licence the patented technology exclusively only in a specific market sector. The company has to pay FBK an amount of money every six months for around three years for the use of the patent. The company will contribute with the payments of the patents in some countries defined in the contract agreement with a fixed percentage. Moreover, the contract states that FBK has to provide further customised services following the company requirements in order to engineer the patented solution.
Impact on organisation	Bring innovation and efficiency to the society.
Comments	A specific clause has been inserted in the contract with the company underling that FBK can use the patented technology for research reasons in any market sector. FBK can exploit the patented technology licensing the technology to other companies in other market sectors. Since FBK is a public institution, the company has to send an official request to start the negotiation with the research centre.

GPI

Case	Founded more than 30 years ago in Trento, over time GPI has constantly grown thanks to significant investments in M&A and to projects developed in partnership with national and international Universities and Research Centres. Since 2018 it has been listed in the Italian stock exchange on the MTA market. In this process GPI has never lost sight of the deepest meaning of its work: creating leading-edge solutions to make health systems sustainable and improve people's quality of life. The integration of software, services and technology, combined with the many years of experience gained working alongside our customers, constitutes a concrete support for innovating treatment models, optimising processes and limiting costs.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	☐ Digital IP ☐ Industrial Process ☐ Product Data ■ SAAS ☐ Cloud ☐ Open Source ☐ AI/ML ■ GDPR
Description	Case is based on a study with a large data set- 8 million records, 20,000 patients, 10 years of depth, Diabetes Clinical Record and Lab. Analysis, Origin from Liguria, Objective: Risk Predictive Model (ML), Model: Gradient Boost Regressor. Challenge is a big number of information. In Italy there are 20 regions with 20 different ways of collecting health data. Company wanted to obtain a pattern recognition of the data that are detectable and independant by their meaning. Four main health targets were idenitfied i.e., glucose, creatinine, diastolic pressure and systolic pressure. Out of these patrons and analysis the company is able to identify the parameters, features impacting target variables as suggested by the clinitians. They were able to train the alghoritms to obtain a high level of prediction. In order to go from research to marketable service they introduced an agent i.e. a web application . Number of variables from laboratory analyises are entered and a live prediction is shown on the risks of the person. This information about the risks is relevant for doctors to start preventive treatment before the symptoms occur with tested person. On the other side by understanding which are the parameters impacting some tartets help change behaviour of patients in order to transform the risks levels of health into lower or moderate levels of risks.
Impact on organisation	Preventive health care and behavioural changes are services enabled by personalised medicine, use of sanitary data and has relevant influence on public health capabilities. Use of personal data, cybersecurity and capacity to elaborate those data are the core aspects of this case.

Go Opti

Case	GoOpti's beginnings date back to 2011. The initial business model included the development of a digital transport market, which GoOpti was also implementing at the time. They offered low-cost road transport of passengers from several Slovenian cities to nearby airports, including in the surrounding countries. They offered several different types of transport on the market and, over time, always new routes, initially with their own vehicles and drivers. As the company found such a business model to be cost-inefficient and, above all, operationally demanding, they began looking for advanced solutions to introduce an innovative business model.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	☐ Digital IP ☐ Industrial Process ☐ Product Data ■ SAAS ■ Cloud ☐ Open Source ☐ AI/ML ☐ GDPR
Description	In 2013, in cooperation with the high-tech company Abelium, they began to develop a new system designed in the form of SaaS (Software as a Service), supported by cloud services and intended for digital support for rapid growth in Slovenia. In early 2015, GoOpti, in collaboration with Abelium and Arhea, prepared and began implementing a digital transformation strategy. The core of the digitally revamped GoOpti is its own innovative SaaS digital marketplace, supported by cloud services, which - in addition to comprehensive support for ticket purchases and daily passenger registration and planning operations - is also dedicated to data-supported business model expansion abroad.
Impact on organisation	Their innovative and market potential was recognized in 2015 by a consortium of international investors, and in 2016 we were supported by the European Agency for Small and Medium Enterprises (EASME) under the H2020 SME Instrument (Phase 2) and financially supported by the Digital Renewal Business GoOpti models in foreign markets. With the internationalisation of the business model in 2018, they have completed the digital transformation of the company - from transport service provider to on-demand mobility platform (business model change). The GoOpti platform offers benefits to passengers, partners, franchisees, carriers and drivers. Franchisees and carriers got rid of the need to find customers, sell and support customers, issue invoices and run settlements by joining the GoOpti platform, as the system does this for them. Drivers also have a mobile application that allows them to check driving data, inform passengers about possible delays and complete a travel order after transport. The system also selects carriers and drivers to run automatically, taking into account parameters such as the estimated cost of transport, the distance to the transport location, the number of journeys per month, the duration of the journeys and the working time of the drivers. "Transport companies triple their revenues by joining our platform. According to company data, each transport company carries an average of more than 360 passengers a month from the GoOpti platform and generates 10 thousand euros in revenue. There are three types of transport available to passengers, tailored to their time availability, desire for in-vehicle privacy and financial means. GOoPTI transport is a unique low-cost service in which passengers with similar wishes regarding the time of departure or arrival are united in the same vehicle. "When booking, the passenger selects a flexibility window from which he can be picked up, and the day before the transport he is informed of the exact transport time, which is within the selected time window." purchase.

Impact on organisation	The service is ideal for users who want to know the actual time of departure when buying a transport. VIP is a private transport on any route. It is the best solution for companies and individuals who want completely private transport at an affordable price. The exact time of departure is determined by the user in the purchase process. Analyzes show that using GoOpti saves an average of 80 euros and 1 hour of time while travelling, while expressing a very high level of satisfaction. With our advanced solutions we can also join the multimodal transport system in the cities, within which GoOpti offers on-demand transport services.
Comments	Source of information: IKT Horizontal network, Smart cities and societies

Event Registry

Case	Event Registry is a SaaS platform that offers global media monitoring and media intelligence. It collects news from over 150.000 news sources in over 80 languages
Main Topic	■ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	■ Digital IP ☐ Industrial Process ☐ Product Data ■ SAAS ☐ Cloud ☐ Open Source ☐ AI/ML ☐ GDPR
Description	All news is semantically annotated and categorised using state-of-the-art NLP tools. By identifying regularities in the news, it also identifies world events that are discussed in the media. The users can: ■ Search for news and articles using over 15 different types of filtering (keywords, concepts, location, source, language, sentiment, ...) ■ Visualise and aggregate the results in several ways offering intuitive ways to identify interesting trends and patterns ■ Reduce the content overload by merging articles discussing the same thing into events ■ Access the data also through the API The service is used for risk management, supply chain monitoring, KYC, and for brand analysis.
Impact on organisation	Information provided by Event Registry can offer an insight into the trends and movements in the society, understanding of world events and their relations between them.
Comments	Core focus points of the company's business models with implication on the digital IP management are the data collection strategy and the information extraction.

Guardiaris d.o.o

Case	Guardiaris is producing custom-designed indoor and outdoor simulators for defence, law enforcement and civilian customers. One of key Guardiaris products in the civil market is the Driver's Response Analytics System (DRAS). With its cutting-edge gaze tracking system, DRAS is a perfect tool assisting in new and existing motorway infrastructure planning. DRAS gives a new perspective in the world of virtual driving simulators and motorway infrastructure planning.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	■ Digital IP ☐ Industrial Process ■ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ☐ AI/ML ☐ GDPR
Description	Company combines data analytics (from various sources such as monitoring events on digital replicas, digital simulation of the real life situations and points of interest of trainees) with the image generation and simulation software registered under the GUARD trademark. GUARD enables real-time rendering of highly realistic terrains and environments, dynamic weather and time-of-day simulation. It uses advanced AI, true-to-life vehicle dynamics and accurate combat situations. Guardiaris has patented a non-laser-based solution, which gathers motion data at an incredible level of detail. This technology allows full freedom of movement, determines exact position, orientation, movement, and enables precise training events in real-time. Gathered data is instantly available for analysis, resulting in rapid adaptation and personalization of the training process.
Impact on organisation	■ Bottom up and concurrent design approach. ■ Core technology for simulator digital twin 3D space orientation - patent (SAS). ■ Data collection on multiple platforms, compatible. ■ Data analytics and presentation (training events, eye tracking, body movement, skeleton) with straightforward user interface: After Action Review (AAR). ■ Fast paced continuous improvement: algorithms - performance - functions - listen to customer requests.
Comments	■ Beyond paper and questionnaire data collection. ■ Training analytics required, must be based on quantitative data, real time collected on training set ■ Development of post training data analytics systems. ■ Tight integration with existing and future product portfolio of training digital twins and own simulation engine (SATT). ■ Internal team of mechanical, electronics, SW, data analytics engineers. ■ Concurrent engineering, drive multiple parallel design paths. ■ Broaden IP portfolio.

QLECTOR LEAP

Case	QLECTOR LEAP uses artificial intelligence methods and, in this way, builds the digital twin of the entire value chain of the manufacturing company: from production to logistics and sales. The digital twin provides a comprehensive operational overview of the entire chain, a prediction of how the chain will change in the next hours, days, weeks and months, and automatic anomaly detection that significantly affects KPIs.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	■ Digital IP ☐ Industrial Process ■ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ■ AI/ML ☐ GDPR
Description	QLECTOR LEAP enables the automation and robotization of tasks that have been in the domain of white-collars, and cannot be solved with existing IT solutions without artificial intelligence methods. QLECTOR LEAP makes users with robotization of tasks more efficient so that (a) they can be more efficient at work because of a comprehensive view of the current and future state of the value chain, and (b) they cover more of the chain than they have so far with less labour.
Impact on organisation	QLECTOR LEAP is unique because it uses machine learning to automatically calibrate parameters. As a result it reduces implementation time from 6 to 2 months compared to competition. Digital twin is used to generate predictions based on actual capacities and efficiency so there is no need for manual calibration during the operation, which reduces maintenance costs.
Comments	Focus points: industry 4.0, digital twin

Solvesall - MACH

Case	MACH (Mobile AI Communication Hardware) is a hardware-software ecosystem that offers connectivity, monitoring and remote control of recreational vehicles.
Main Topic	☐ Legal aspects ☐ IP Agreement ■ Business Model
Specificities	☐ Digital IP ☐ Industrial Process ■ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ■ AI/ML ■ GDPR
Description	By installing the hardware, the vehicle is converted into a smart-home + smart office on the wheels. Users get access to all the data, and the ability to control all of the appliances (heating, AC, batteries, water, lights, etc.) over their smartphones. The users also gain access to caravanning related points of interest data. Besides end-users, mobile unit manufacturers and rental companies gain access to the fleet and product analytics and gain a channel to the end user and ability to follow the product throughout the whole lifecycle. The anonymized data from connected vehicles is also used by the AI algorithms, to automatically learn relevant points of interests and available resources (water, electricity, waste facilities). This greatly reduces the data maintenance, because it is automated.
Impact on organisation	■ On Company: Information provided by MACH offers ability to make data supported product decisions, based on the usage of the mobile units. ■ On Society: Information provided by MACH offers the ability to contribute to the circular economy of the products and reduce the CO2 emissions by driving when searching for clean water, waste water/dark water facilities.
Comments	MACH is already installed over more than 2000 vehicles, and we are gaining approximately 10k of new connected vehicles per year.

IP related management in organisation merger or acquisition

Case	MACH (Mobile AI Communication Hardware) is a hardware-software ecosystem that offers connectivity, monitoring and remote control of recreational vehicles.
Main Topic	■ Legal aspects ☐ IP Agreement ☐ Business Model
Specificities	■ Digital IP ■ Industrial Process ■ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ☐ AI/ML ☐ GDPR
Description	The 2 companies constituting this case subject are two companies strongly interrelated and funded by the same people, the first one developing a software and the second commercialising this software on the market. The IP on the software therefore was completely owned by the first company that was in charge of the development and no agreement between the two parts was in place regulating the revenues from the commercialization business of the second company. When the software development company was sold, due diligence topic became urgent. To address the issue a licence agreement was put in place in order to give note that this mode of contractual relationship was already implemented with an agreement not written but verbal and that in that historical moment was given note of the past and regulate the future.
Impact on organisation	Potentially the company could have seed the failure of the acquisition from a third company inducing relevant consequences.
Comments	Relevance of the IP related agreements and of the due diligence process is of maximum importance when companies are in a reorganisation, acquisition or merger phase. The due diligence should be clearly addressed in complex company interrelations and all the agreements supporting the business implementation should be prepared from an early stage.

Employees transfer and IP

Case	MACH (Mobile AI Communication Hardware) is a hardware-software ecosystem that offers connectivity, monitoring and remote control of recreational vehicles.
Main Topic	■ Legal aspects ☐ IP Agreement ☐ Business Model
Specificities	■ Digital IP ☐ Industrial Process ☐ Product Data ☐ SAAS ☐ Cloud ☐ Open Source ☐ AI/ML ☐ GDPR
Description	A company working on third party test services is in the process of managing an employee resignation and required to define a Resignation and General Release Agreement. To this purpose the company mapped the possible IP that could be exploited by eventual competitors during the transfer of the employee. The first idea was that the company didn't have any relevant IP. During a second iteration, it emerged that all the methodologies set up during years of tests in the company are the crucial IP protected under the trade secret in the company. And were then subject of the resignation agreement.
Impact on organisation	The risk for the company to have their trade secrets disclosed and unprotected as a consequence of an employee transfer to a competitor is relevant and needs attention and proactive management.
Comments	Not all the IP is related to patents, copyrights etc. Other IP connected with industrial secrets is equally relevant and crucial to preserve the competitiveness of the company. The IP that is behind e.g. methodologies, client lists, suppliers, commercial agreements etc. is equally relevant and must be evaluated and be subject of agreements between the company and its former employee.