DE TULLIO & PARTNERS
INTELLECTUAL PROPERTY ATTORNEYS

NEW CHALLENGES FOR HIGH INNOVATIVE COMPANIES: DATA PROTECTION, TRADE SECRETS AND CYBER-SECURITY

January 25, 2018

Avv. Elio De Tullio

Agenda

- *The EU Regulation 679/2016 (General Data Protection Regulation - GDPR)*
- *How to protect data (personal and confidential) in a company*
- *Cyber-security: overview*
- *Innovation & Trade secrets*
- *Protection of Trade secrets: the new EU Directive 2016/943 and the US Defend Trade Secret Act*
- *Data protection and companies: applications context*
- *New requirements: an opportunity for companies to improve their competitiveness*
- *Conclusions*

The EU Regulation 679/2016 (General Data Protection Regulation - GDPR)

- The year 2018 will entail profound changes for companies with high innovative potential which operate globally, particularly for SMEs.

- First of all, by May 2018, European companies will have to adapt to the new requirements introduced by the EU Regulation 679/2016 (better known as *General Data Protection Regulation - GDPR*) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

- Such Regulation introduced several changes in relation to privacy and data protection rules.

Main changes

- Tougher fines
- **Scope**: all companies, even those located outside the EU, must comply with GDPR where they offer goods or services to individuals within the EU or monitor the activity of people within the EU
- Accountability requirements
- **Data processors**: they will be submitted to specific obligations, including those to implement appropriate security standards, ensure adequate record-keeping and inform the data controller of any breach.
- **Contract obligations**: a number of new provisions must be included in all contracts involving the processing of personal data. This may involve changes of existing commercial arrangements.
- **Data Protection Officer (DPO)**: in some circumstances a DPO will need to be designated by the data controller or processor.
- Consent
- Data subjects rights

Overview of the main changes adopted by the GDPR 1/4

- **EXTENSION OF THE TERRITORIAL SCOPE**:

The new Regulation will apply to all processing of personal data carried out by companies operating in the EU, regardless if such activity takes place in the EU or not. Moreover, it will also apply to all companies processing personal data of subjects residing in the EU, regardless the location of the company if the activities are related to "*a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union*" (**Article 3**).

- **STRENGTHENING OF CONDITIONS FOR CONSENT**:

According to the GDPR (**Article 7**), the conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Overview of the main changes adopted by the GDPR 2/4

- **NOTIFICATION AND COMMUNICATION OF DATA BREACH**:

If there is the high risk that the data breach may affect "*the rights and freedoms of natural persons*", the controller shall without delay (within 72 hours after becoming aware of the breach) notify the breach to the supervisory authority (**Article 33**) and communicate the same to the data subject (**Article 34**).

- **DATA PROTECTION IMPACT ASSESSMENT and DATA PROTECTION OFFICER**:

Companies are required (**Article 35**) to carry out a prior assessment of the impact of the processing in case it may result *in a high risk to the rights and freedoms of natural persons,* with the advice of the Data Protection Officer (DPO).

In particular, the DPO (**Articles 37, 38 and 39**) is a new business figure which will ensure and manage the adequate use of personal data by companies. Appointing a DPO will be mandatory only for public authorities or bodies and in case the core business of processors/controllers is to carry out processing activities which require *regular and systematic monitoring of data subjects on a large scale* or activities related to particular categories of data or data on convictions and offences.

Overview of the main changes adopted by the GDPR 3/4

- **DATA PORTABILITY**:

The GDPR introduced the right to data portability (**Article 20**), i.e. the right for a data subject to receive data concerning it in order to forward them to another controller. Moreover, the personal data may be transmitted directly from one controller to another, if it is possible.

- **PENALTIES**:

The GDPR adopted an accurate penalty system. In general, in case of non-compliance with the new rules, the sanctions can amount up to 20 million EUR or 4% of the worldwide annual turnover (**Article 83**). Moreover, legal actions may also be initiated in the form of class actions by customers or other persons damaged by unlawful processing.

Overview of the main changes adopted by the GDPR 4/4

- **PRIVACY BY DESIGN and PRIVACY BY DEFAULT**:

According to Article 25 "*the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects*." At the same time, the controller shall ensure through appropriate technical and organizational measures that *only personal data which are necessary for each specific purpose of the processing* will be processed by default.

New requirements and precautions for companies

- The consent to the processing of data must be updated;
- The data controllers must adopt appropriate measures to provide the data subject with all the information and communications relating to the processing in a direct, transparent, intelligible and easily accessible form, with a simple and clear language;
- The data protection policy must be updated and implemented;
- The exchange of personal data with third countries (i.e. non-EU States, therefore probably also UK) will be subject to strict rules;
- In case of exchange or data transferred abroad, in a third country classified as unreliable, adequate guarantees or authorizations will be necessary;
- Similar precautions will be required also in case of online data storage (i.e. Cloud data storage);

How to protect data (personal and confidential) in a company

- Develop guidelines or *vademecum* in relation to the processing procedure;
- Create and implement protocols and internal procedures in order to strategically manage the data (i.e. **Privacy Policy and, as we will se afterwards, a possible Trade Secrets Policy**);
- Organize training session for the staff in order to make them aware of the importance of data protection.
- Create and implement an internal department which deals with data protection.
- Use cyber-security measures in order to improve the protection of data.

Data protection and companies: an example of interaction

- Data can be personal or not personal (i.e. trade, commercial or business information).
- Personal data are protected and regulated by Privacy law whereas commercial or trade information are regulated by trade secret related laws. **However, often personal data can assume relevance also in relation to trade secret protection**.
- This is the case, for example, of a **database including lists of clients or distributors**. In fact, such lists could be important for companies, especially if consisting in an advanced database and not in a simple list. In particular, such database can include customers personal data and contact details (name, address, telephone number, date of birth, banking details…) but also customers' preferences or the methods of supply in relation to specific clients.
- **In this circumstances, a database or a list of customers are subject to privacy protection and they also constitute trade secrets**. Therefore, measures that the company adopts to such database or lists according to privacy regulation are also important in relation to trade secrets protection. In particular, these security measures can be useful during a lawsuit in order to persuade the judge to protect the database as a trade secret.

Case study – Using cyber-security measures to protect data

- In a recent Austrian case*, the plaintiff and the defendant were competitor companies with the same customers. The plaintiff also provided its clients with an Internet server for the storage of their clients' data. This server was protected by a logging system (i.e. user name and password).

- A defendant's employee was able to illicitly have access to such server bypassing the password. During its defense, the defendant argued that such data were not trade secrets since they could be easily accessible.

- However, the Court ruled that such data were kept confidential through the logging system and that the fact that the security system of the plaintiff was not successful does not mean that the owner had no interest in keeping the information confidential or that he did not take reasonable steps to maintain such data secret.

- **The will to keep the information secret can be assumed also from the behaviour of the owner. The existence of a logging system demonstrates that only a restricted number of people had access to the server.**

*Austria Supreme Court, Decision N. 4 Ob 165/2016t

Cyber-security: overview

- Improve technological data protection infrastructures can result to be crucial for a company in relation to data protection.

- In fact, recent data* have shown that industrial secrecy is one of the main targets of cyber-attacks and it has been estimated that in recent years such illicit attacks, as well as attacks related to other intellectual property rights, have seen an increase of around 60%.

- The authors of such cyber-attacks usually seize companies' data and documents and ask to be payed in order to receive back data.

*Klahr et al., Cyber Security Breaches Survey 2016, at 1 (May 2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf

Cyber-security measures 1/2

- **IDENTIFY AND CONTROL ACCESS TO DATA**:
  - ✓ **Password and username system**: this is the simplest and basic way to protect data.
  - ✓ **Limited access**: limiting access to data only to some specific subjects can improve the security of data.
  - ✓ Secure data on a **server storage** and protect the server.

- **NETWORK AND COMPUTER PROTECTION**:
  - ✓ **Block the access to dangerous websites**: in this way it could be possible to avoid the risk of viruses or undesirable programs in the computer network.
  - ✓ **Firewalls and antivirus programs**: the installation and the use of antivirus programs increase the data protection and reduce the risk of data loss.
  - ✓ **Encoding and encryption of data**: in this way it is possible to increase data protection and better monitor the disclosure of the same.

Cyber-security measures 2/2

- **MONITORING OF EMAIL and CLOUD STORAGE**:
  - ✓ In this way it is possible to better monitor the distribution and the disclosure of data.

- **RESTRICTION OF DATA STORAGE/DISTRIBUTION**:
  - ✓ **Controls on printing, distribution or modification of documents including data**: in this way it is possible to better monitor the distribution of data.
  - ✓ **Restrict/prohibit the use of USB storage**: prohibiting or limiting the use of USB (or other memory devices) can increase the protection of data.

Innovation & Trade secrets

- Nowadays every innovation arises with a data, which is usually an electronic data, stored in a PC.
- Companies can adopt a trade secret based approach and/or a patent based approach; such models are complementary.
- In particular, data and documents related to the first phase of research and development of the innovation (before it might be considered an invention) are generally protected as trade secret.
- In a second moment, the inventor can decide how to protect and valorize the invention (i.e. as Trade Secrets, Patent or other instruments);
- In any case it is always necessary to make clear the link between research and development costs of the innovation and the innovation itself, also in terms of tax incentives (i.e. Patent Box).

Protection of Trade secrets: the new EU Directive 2016/943 and the US Defend Trade Secrets Act

- In general, trade secrets are business information (protected by reasonable safety measures) which have a commercial value for the owner due to their confidential nature.

- For example, the following information can be considered trade secret:

- ✓ *know-how;*
- ✓ *technical, commercial, operational and/or financial information;*
- ✓ *confidential email and correspondences;*
- ✓ *production and manufacturing processes (i.e. method of production);*
- ✓ *company's strategies (i.e. business method, marketing plans, sales, quantities produced, acquisitions, contractual offers…);*
- ✓ *customer lists;*
- ✓ *recipes for specific preparations;*
- ✓ *chemical formula or algorithms;*
- ✓ *designs or prototypes;*
- ✓ *price lists;*
- ✓ *distributors lists;*
- ✓ *internal documents and database…*

Protection of Trade secrets: the new EU Directive 2016/943 and the US Defend Trade Secrets Act

- At EU level, the protection of Trade Secrets is going to be strengthened and harmonized across the Member States thanks to the implementation of the Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 (hereinafter, “EU Directive”).

- Pursuant to Article 19 of the EU Directive, in Italy, as well as in the other Member States, the Directive is expected to be implemented by June 9, 2018.

- It has to be noted that the EU Directive was adopted in the same period of time of the approval of the *Defend Trade Secret Act* in the United States.

The EU Directive 2016/943 on Trade Secrets 1/4

- The Directive 2016/943 aims at:
  - ✓ Providing a **consistent definition of "trade secret"** and how it can be protected;
  - ✓ Setting out the **remedies** to be adopted in the event of a misuse of a trade secret;
  - ✓ Ensuring that **national courts can prevent disclosure** of trade secrets during legal proceedings.

- The Directive also aims at providing a **minimum level of protection** to trade secrets, allowing Member States to apply stricter rules.

- It also establishes **a common set of principles, definitions, procedures, safeguards and remedies** that must be applied across the EU.

The EU Directive 2016/943 on Trade Secrets 2/4

- Currently, there are relevant differences between the different EU Member States and this creates confusion and difficulty in protecting trade secrets.

- In general, the protection of trade secrets does not arise from registration and it is potentially unlimited in time.

- **Sweden** has a specific law on trade secrets (the Trade Secret Act of 1990) which provides explicit definitions of trade secrets, offenses and sanctions relating to their violation and also provides specific criteria for compensation of damages.

- **Italy** and **Portugal** introduced a definition of trade secrets in their respective Industrial Property Code.

- Most of the other Member States introduced provisions in their civil or criminal laws, also in relation to unfair competition or common law principles.

The EU Directive 2016/943 on Trade Secrets 3/4

- The new EU Directive contains provisions in relation to its object and scope of application, as well as definitions.

- Furthermore, it also regulates the lawful use or acquisition of trade secrets (i.e. independent discovery or the so called "*reverse engineering*"), the corrective measures, remedies and sanctions in case of infringement.

- In particular, Article 2 of the EU Directive provides for the following **definition of trade secret**:

  "*information which meets all of the following requirements:*

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

  (b) it has commercial value because it is secret;

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

The EU Directive 2016/943 on Trade Secrets 4/4

- Article 3 regulates the "***lawful acquisition, use and disclosure of trade secrets***" in case the trade secret is obtained by:

  "(a) independent discovery or creation;

  (b) observation, study, disassembly or testing of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer of the information who is free from any legally valid duty to limit the acquisition of the trade secret;

  (c) exercise of the right of workers or workers' representatives to information and consultation in accordance with Union law and national laws and practices;

  (d) any other practice which, under the circumstances, is in conformity with honest commercial practices.

  2. The acquisition, use or disclosure of a trade secret shall be considered lawful to the extent that such acquisition, use or disclosure is required or allowed by Union or national law."

The US Defend Trade Secret Act (DTSA) 1/2

- The Defend Trade Secret Act was signed on May 11, 2016 by the President Obama.
- This Act provided for a trade secret protection at **federal level** but did not repeal the national legislations on the matter. However, with the entering into force of such Act, companies can choose to initiate a federal legal proceeding if the infringement relates to more than one State.
- According to the DTSA, companies can request the Federal Court to issue **provisional measures**, including seizure in case it is necessary to preserve evidence or prevent the disclosure of trade secret.
- Moreover, the new Act provides for **compensation for damages**; damages can be calculated on the base of actual loss, unlawful enrichment or reasonable royalty and the compensation could be increase in case of bad faith.

The US Defend Trade Secret Act (DTSA) 2/2

- Another relevant innovation is the **whistleblower immunity**, set forth in Section 7(a):

"An individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that ''(A) is made ''(i) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and ''(ii) solely for the purpose of reporting or investigating a suspected violation of law; or ''(B) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal.".

* Source: https://www.congress.gov/114/plaws/publ153/PLAW-114publ153.pdf

Data protection and companies: applications context

- It is necessary for companies to understand that data fulfillments are important for several reasons.
- In fact, privacy compliance - a burden and a cost for the company – can be a competitive advantage in terms of trade secrets protection.
- The privacy obligations can be useful in case of lawsuits in order to protect the company.
- In fact, measures that the company adopts to protect data (and, therefore, avoid their dissemination) can be important tools in a lawsuit as evidence of the adoption of reasonable measures to keep information secret.
- Finally, the implementation of data protection requirements could also be a useful tool for innovative companies in order to get easily access to tax concessions instruments or other financial instruments provided by EU legislation.

Europe 2020 strategy and Horizon 2020 1/2

- Data protection through the Data Privacy Regulation and the Directive on Trade Secrets should be seen in the overall context of the EU project called **Europe 2020**.

- **This project aims to encourage companies to invest in innovation, providing them with the tools necessary to protect ideas and innovations, based on the assumption that such ideas and innovations are incorporated, in most cases, into confidential and secret electronic data.**

- In particular, Europe 2020 has three priorities: *smart growth, sustainable growth and inclusive growth*. In the aim of such priorities, the objects of the project are related to occupation, research and development (R&D), poverty and social exclusion, education and climate change and energy.

- **As regards the R&D target, such project includes several strategies and activities aimed to the development of innovation and technologies**; said activities and strategies are also improved at EU Member States national level.

Europe 2020 strategy and Horizon 2020 2/2

- In the context of the Europe 2020 strategy aimed to the development of innovation and technologies, the SMEs instrument Horizon 2020 provides for a full-cycle business innovation support. It has three phases, including a coaching and mentoring service.

- The SMEs instrument is part of the European Innovation Council pilot (EIC pilot). This was launched on 27th October 2017 as part of the *Horizon 2020 Work programme 2018-2020*, together with the Fast Track to Innovation (FTI), Future and Emerging Technologies (FET) Open and Horizon Prizes.

- Such SMEs instrument offers Europe's high-innovative SMEs the chance to get funding for breakthrough ideas with a market-creating potential.

Industry 4.0 (or Economy 4.0) programs

- **In general, "Industry 4.0" means the fourth Industrial Revolution and it is the process which lead to the automatization of the industrial production through the interconnection of new technologies and machines.**

- Some EU States (e.g. Italy, France, Germany, UK, The Netherlands) adopted in recent years strategical programs called "Industry 4.0" in order to promote and support the development of technologies and innovation.

- In particular, such programs provide for financial incentives, tax credits for research, tax benefits for investments in *start-up*, tax deductions, subsidised loans, financing operations etc.

- One of the principal action in the light of the "Industry 4.0" programs is the so-called "**Patent Box**", already applied in many EU countries under the OECD Guidelines. This tool introduced an optional tax regime for those revenues arising from IPRs, creative works and information, process and formula related to industrial, commercial or scientific matters, which can be protected according the law.

Patent Box in the European Union

- The so-called “Patent Box” is already applied in several EU Member States (i.e. Italy, France, Belgium, The Netherlands, Hungary, Ireland, Spain, Portugal, UK, Malta, Luxembourg and Cyprus).

- The following tables include data* on tax regime and exemption of net income applied in some of EU Member State which already provide for Patent Box or similar systems.

	Italy	France	The Netherlands	Belgium
Tax regime	13,9 %	15,5 %	5 %	5 %
Exemption of net income	50 %		80 %	85 %

	Ireland	Spain	Portugal	Hungary	UK
Tax regime	6,25 %	10 %	14,75 %	9 %	10 %
Exemption of net income	50 %	60 %	50 %		50 %

*Source: STS-Deloitte

New requirements: an opportunity for companies to improve their competitiveness

- If the compliance required by the aforementioned legislative instruments will be managed strategically by companies that operate globally – hence also those that intend to maintain partnership relations with European and/or US companies – such undertakings may push companies to create and implement protocols and internal procedures in order to strategically manage the data and, where the relevant conditions are met, protect them as trade secrets and intellectual property rights, as well as enhancing them from an economic point of view.

- In such respect, companies will be called upon to act on three fronts:
  - ✓ implementing their organizational models and identifying managerial figures in charge with the data management and trade secret protection;
  - ✓ studying and adopting contractual models of non-disclosure in connection to business relationships with third parties;
  - ✓ adapting its technological data protection infrastructures (i.e. cyber-security).

Confidentiality agreements or clauses

- Signing **non-disclosure agreements** or including **confidentiality clauses** into contracts with employees or third parties are effective ways to better protect data dissemination.

- In particular, such confidentiality agreements or clauses might shall have the following characteristics:
  - ✓ state clearly which information (i.e. trade, personal, technical data etc.) **constitutes confidential data and belongs to the company**;
  - ✓ define the **limits of the use** of confidential information (i.e. only if such use is necessary for carrying out the work);
  - ✓ require employees or third parties to take **all reasonable measures** in order to protect confidential data;
  - ✓ prohibit the use of **confidential information acquired from a previous employer or experience**;
  - ✓ limit the **printing and distribution** of documents including confidential data (i.e. possible only with the consent of the owner);
  - ✓ provide that confidential data must be **returned to the company** in case of termination of the employment or contract.
  - ✓ provide for an **extension of the non-disclosure obligation** even after the termination of the employment or contract.

Conclusions

- Companies must consider the new EU GDPR as an opportunity to improve their competitiveness and business value.
- Moreover, in light of the interaction between the protection of personal data and trade secrets, the possibility to appoint a Data Protection Officer, if needed, can push companies to consider the creation of an IP Officer (with competences in Trade Secrets and other IP rights), i.e. **new professional figures of Innovation Managers**.
- Therefore, implementing the organizational model of a company through the inclusion of such managerial figures, can enhance the company's value from an economic and strategic point of view.
- Only by means of a virtuous interaction between the above outlined aspects, innovative companies will be able to successfully meet the challenges of the future.

iam presents

IPBC® Europe

HARNESSING IP VALUE IN EUROPEAN COMPANIES

MARCH 20-21 2018 AMSTERDAM

Learn from and connect with like-minded experts leading IP innovation at Europe's most forward-thinking organisations – all gathered together in one place.

An exclusive discounted rate of €590 is available for SMEs, which are members of INSME.

Register with code INSME590 at www.IPBCEurope.com to save €360 on the full rate.

THANK YOU FOR YOUR ATTENTION!

Avv. Elio De Tullio

DE TULLIO & PARTNERS
INTELLECTUAL PROPERTY ATTORNEYS

E-mail: info@detulliopartners.com

www.detulliopartners.com