THE REG. (EU) 2019/881 AND THE REG. (EU) 2016/679

CYBERSECURITY ACT / GDPR

EXAMINATION INTERACTION POINTS

Index

Title _____ Pag.

FOREWORD

Taking a cue from the principles enunciated in the recitals listed below, I wanted to highlight the key points of the origin of my analysis.

Recitals 1 and 2 of Reg. (EU) 2016/679 cite:

> *(1) The protection of natural persons in relation to the processing of personal data is a fundamental right .....*
>
> And again
>
> *(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, ...*

Recitals 2 e 3 of Reg. (EU) 2019/881 cite:

> *(2) ... Digitization and connectivity are becoming core features in an ever growing number of products and services and with the advent of the internet of Things (IoT) an extremely high number of connected digital devices are expected to be deployed across the Union during the next decade. While an increasing number of devices is connected to the internet, security and resilience are not sufficiently built in by design, leading to insufficient cybersecurity. In that context, the limited use of certification leads to individual, organisational and business users having insufficient information about the cybersecurity features of ICT products, ICT services and ICT processes, which undermines trust in digital solutions. ..*
>
> *(3) Increased digitization and connectivity increase cybersecurity risks, thus making society as a whole more vulnerable to cyber threats and exacerbating the dangers faced by individuals, including vulnerable persons such as children. In order to mitigate those risks, all necessary actions need to be taken to improve cybersecurity in the Union so that network and information systems, communications networks, digital products, services and devices used by citizens, organisations and businesses – ranging from small and medium-sized enterprises (SMEs), ...*

GOAL

The purpose of my analysis is not to express an academic exercise but to provide a practical tool that allows to understand the points of interaction between the two laws and the practical impacts, these necessary for the performance of both legal and technical activities.

In the following paragraphs, I have reported a summary table that, against a topic, highlights the articles in which this topic is treated in both laws.

Subsequently, I reported in detail the articles of the law highlighting in red the key aspects of the analysis.

RECAP

Both regulations present logical interactions that need to be examined.

The table below summarizes the articles of law that highlight logical and practical concepts that are closely related.

CROSS REFERENCE		
ARGUMENT	REG. (EU) 2019/881 CYBERSECURITY ACT *Articles*	REG. (EU) 2016/679 GDPR *Articles*
SECURITY	1 *in particular; all law;*	5; 32; 35; 40; 45;
RELIABILITY LEVEL	*CONCEPTS: basic, substantial, high* 2; 52; 53; 54;	32;
RESILIENCE	1; 4;	32;
RISK	5; 52;	33; 34; 35; 40;
BY DESIGN	51;	25;
CERTIFICATION AND COMMISSION	56;	24; 42; 43;
PENALTIES	65;	83; 84;

TABLE OF RECAP

DETAIL

ARGUMENT: *SECURITY*

REG. (EU) 2019/881	REG. (EU) 2016/679 GDPR
Article 1 – Subject matter and scope *1. With a view to ensuring the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience and trust within the Union, this Regulation lays down: ....*	Article 5 - Principles relating to processing of personal data *1. Persona data shall be:* *lett. (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures («integrity and confidentiality»).* Article 32 – Security of processing *1. ..... the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, ...* *2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.* Article 35 – Data protection impact assessment *7. The assessment shall contain at least:* *lett. (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance...* Article 40 - Codes of conduct *2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, ... to:* *lett. (h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;* Article 45 - Transfers on the basis of an adequacy decision *1. A transfer of personal data to a third party ....* *2. When assessing the adequacy of the level of protection, ... of the following elements:* *lett. (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, ...*

Consideration

In both laws, security is the main point. The GDPR considers this point to be the instrument to guarantee personal data, while 2019/881 extends the perimeter also to all data and treatments belonging to the system also composed of Information Communication Technologies.

ARGUMENT: RELIABILITY LEVEL

REG. (EU) 2019/881	REG. (EU) 2016/679 GDPR
Article 2 - Definition *(21) «assurance level» means a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme ....* Article 52 - Assurance levels of European cybersecurity certification schemes *1. A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services and ICT processes: «basic», «substantial» or «high». The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident.* *2. European cybersecurity certificates and EU statements of conformity shall refer to any assurance level specified in the European cybersecurity certification scheme ...* *5. A European cybersecurity certificate or EU statement of conformity that refers to assurance level «basic» shall provide assurance that ... statement of conformity is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks ..* *6. A European cybersecurity certificate that refers to assurance level «substantial» shall provide assurance that .... issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources ....* *7. A European cybersecurity certificate that refers to assurance level «high» .... issued meet the corresponding security requirements ...* Article 53 – Conformity self-assessment *1. ... conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, ICT services or ICT processes. Conformity self-assessment shall be permitted only in relation to ICT products, ICT services and ICT processes that present a low risk corresponding to assurance level «basic».* Article 54 - Elements of European cybersecurity certification schemes *1. European cybersecurity certification scheme shall include at least the following elements:* *b) a clear description of the purpose of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme;*	Article 32 – Security of processing *1. Taking into account the state of the art, ..., the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:* *b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;* *c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*

Consideration

The 2019/881 introduces:

1. *the concept of "reliability" in three contexts: product, service and process; this principle correlates with "ensuring an adequate level of safety to the risk" described in article 32 of 2016/679;*
2. *the definition of «basic», «substantial», «high» reliability;*
3. *the principle of "conformity";*
4. *the principle of "responsibility of the manufacturer or provider" of products, services or processes; this principle is of fundamental importance for triggering a change of mentality in the economic-social system.*

ARGUMENT: *RESILIENCE*

REG. (EU) 2019/881	REG. (EU) 2016/679 GDPR
Article 1 – Subject matter and scope *With a view to ensuring the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience and trust within the Union, this Regulation lays down: ....* Article 4 - Objectives *3. ENISA shall support capacity-building and preparedness ... to increase the protection of their network and information systems, to develop and improve cyber resilience and response capacities, and to develop skills and competencies in the field of cybersecurity.*	Article 32 - Security of processing *1. Taking into account the state of the art, ..., the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:...:* *c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*

Consideration

The 2019/881 introduces: the definition of "cyber resilience"; this principle correlates with the "ability to restore" described in article 32 of 2016/679.

ARGUMENT: *RISK*

REG. (EU) 2019/881	REG. (EU) 2016/679 GDPR
Article 5 - Development and implementation of Union policy and law *ENISA shall contribute to the development and implementation of Union policy and law, by:* *2) assisting Member States to implement the Union policy and law regarding cybersecurity … providing advice and best practices on topics such as risk management, incident reporting and information sharing, …;* Article 52 - Assurance levels of European cybersecurity certification schemes *1. …. The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident..;* *4. .. The certificate … the purpose of which is to decrease the risk of, or to prevent cybersecurity incidents ..;*	Article 33 - Notification of a personal data breach to the supervisory authority Article 34 - Communication of a personal data breach to the data subject Article 35 – Data protection impact assessment *1. Where a type of processing .., is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, ..* *7. The assessment shall contain at least:* *lett. (c) an assessment of the risks to the rights and freedoms of data subject referred to in paragraph 1; and…* *lett. (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data …* Article 40 - Codes of conduct *2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:* *lett. (i) the notification of personal data breaches (accident!) to supervisory authorities and the communication of such personal data breaches to data subjects;*

Consideration

The 2019/881 introduces:

1. *the principle of "risk management"; this principle correlates with the "risk assessment" described in article 35 of 2016/679;*
2. *the principle of "accident reporting"; in the event of an accident it could mean that this principle correlates with the "Notification" described in article 33, with the "Communication" described in article 34, with the "Notification" described in article 33, with the "notification of a violation"described in article 40 of 2016/679;*
3. *the principle of "probability and impact of an accident" and "whose objective is to reduce the risk of cyber security incidents, or prevent them"; this principle correlates with the "Data Protection Impact Assessment" described in Article 35 of 2016/679.*

ARGUMENT: BY DESIGN

REG. (EU) 2019/881	REG. (EU) 2016/679 GDPR
Article 51 – Security objectives of European cybersecurity certification schemes *A European cybersecurity certification scheme shall be designed to achieve, as applicable, at least the following security objectives:* *lett. (i) that ICT products, ICT services and ICT processes are secure by default and by design;*	Article 25 – data protection by design and by default

Consideration

The 2019/881 introduces:

1. *the principle of "design" of systems and "safe from design and by default"; this principle correlates with article 25 of 2016/679.*

ARGUMENT: CERTIFICATION

REG. (EU) 2019/881	REG. (EU) 2016/679 GDPR
Article 56 – Cybersecurity certification	Article 24 - Responsibility of the controller *1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.* *3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.* Article 42 – Certification Article 43 – Certification bodies

Consideration

The principle of "Certification of cybersecurity" of products, services or processes; this principle is of fundamental importance for triggering a change of mentality in the economic-social system.

ARGUMENT: *SANZIONI*

REG. (EU) 2019/881	REG. (EU) 2016/679 GDPR
Article 65 - Penalties	Article 83 – General conditions for imposing administrative fines Article 84 – Penalties

Consideration

CONCLUSION

The examination of the points of interaction, set out above, brings out various principles and among these there are two which I believe, in my opinion, of extreme importance; these principles concern the products, services or processes of ICT.

The two principles are:

1. "Responsibility of the manufacturer or provider ";
2. "Cybersecurity certification";

both principles are of fundamental importance since they are the basis of a trigger of the change of mentality in the economic-social system.

The responsibilities of the manufacturer or supplier impose investments to adopt all the necessary measures for the protection of data and systems, up to pushing the Data Controllers to certify the products, services or processes within the company management system. The companies that will undertake this initiative will most likely increase market positions in the future.

The European Union, with the regulations introduced, has begun to establish a legislative continuity solution that implies duties to protect citizens' rights, as stated in recital 3 of Reg. (EU) 2019/881:

> *"....In order to mitigate those risks, all necessary actions need to be taken to improve cybersecurity in the Union so that network and information systems, communications networks, digital products, services and devices used by citizens, organisations and businesses – ranging from small and medium-sized enterprises (SMEs), ..."*

If it is true that the economic damage is immediately easier to quantify, the damage to the image could in time turn out to be much greater. It is therefore essential for the Controllers to understand that the damage is not limited to others but can involve anyone at any time, with high costs both for the sanctions received and for the damage suffered and caused.

Therefore, the Controllers will no longer be able to remain indifferent and will have to seriously consider the fact that prevention is better than cure.