MSECB

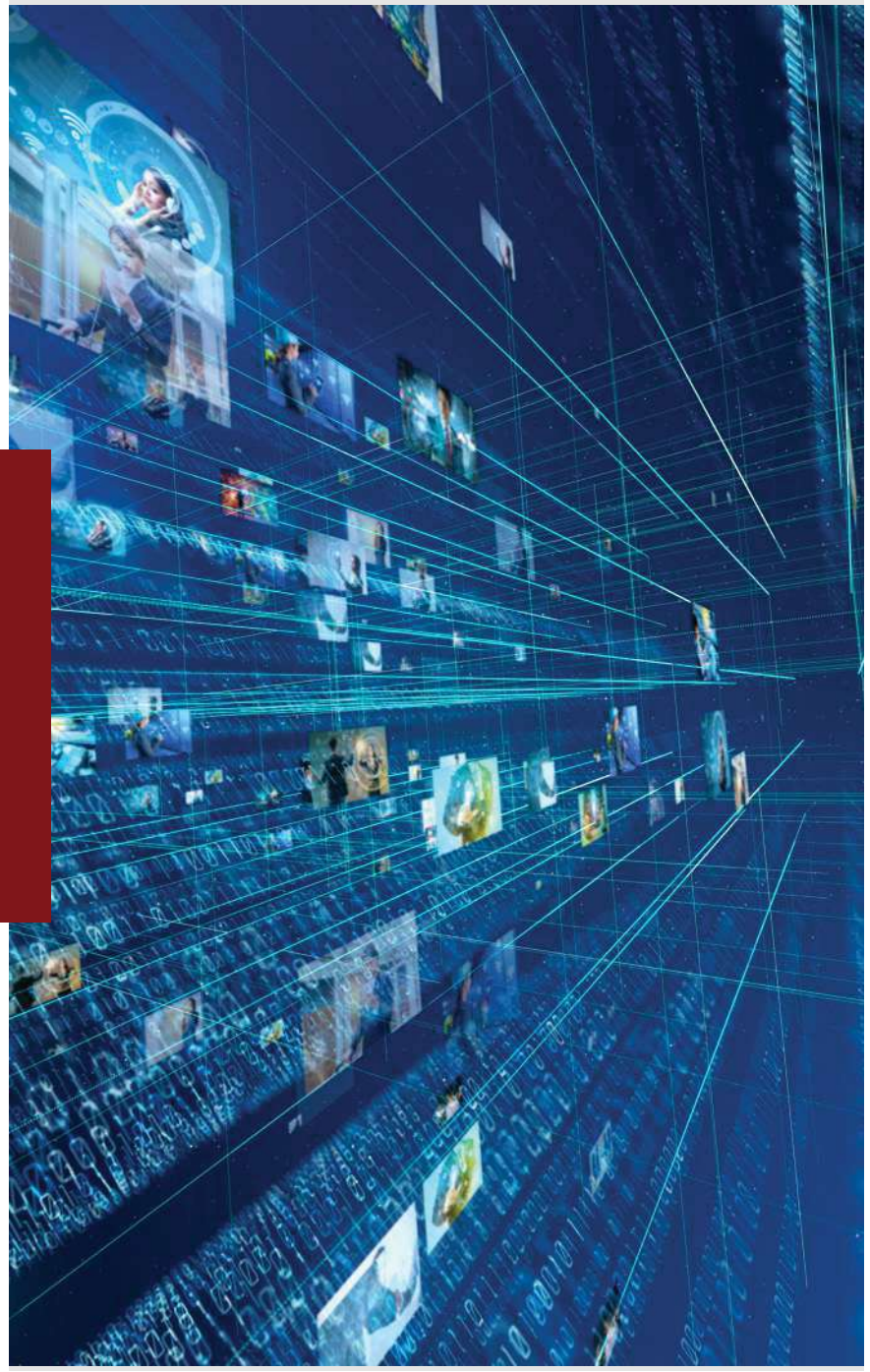
HOW PRIVACY BY DESIGN IS RELATED TO GDPR?

www.msecb.com

What is Privacy by Design?

Privacy by Design is an internationally recognized privacy standard that has been endorsed globally by Data Protection Authorities and Privacy Commissioners, since 2010 (Jerusalem, October 29, 2010). The resolution recognizes Commissioner Cavoukian's concept of Privacy by Design – which ensure that privacy is embedded into new technologies and business practices, right from the outset – as an essential component of fundamental privacy protection. Privacy by Design is structured around 7 Foundational Principles that exist as the baseline robust for data protection.

PbD has existed as a best-practice framework from the 1990s, but few are aware of it, let alone use it. This has changed now with GDPR, which has become legally enforceable in May 2018 that requires privacy by design and by default across all users and applications.



What is the GDPR?

The GDPR is a set of EU laws that is effective from **May 25th, 2018.**

The purpose of the GDPR is to provide a set of standardized data protection laws across all the member countries. This should make it easier for EU citizens to understand how their data is being used, and also raise any complaints, even if they are not in the country where it is located.

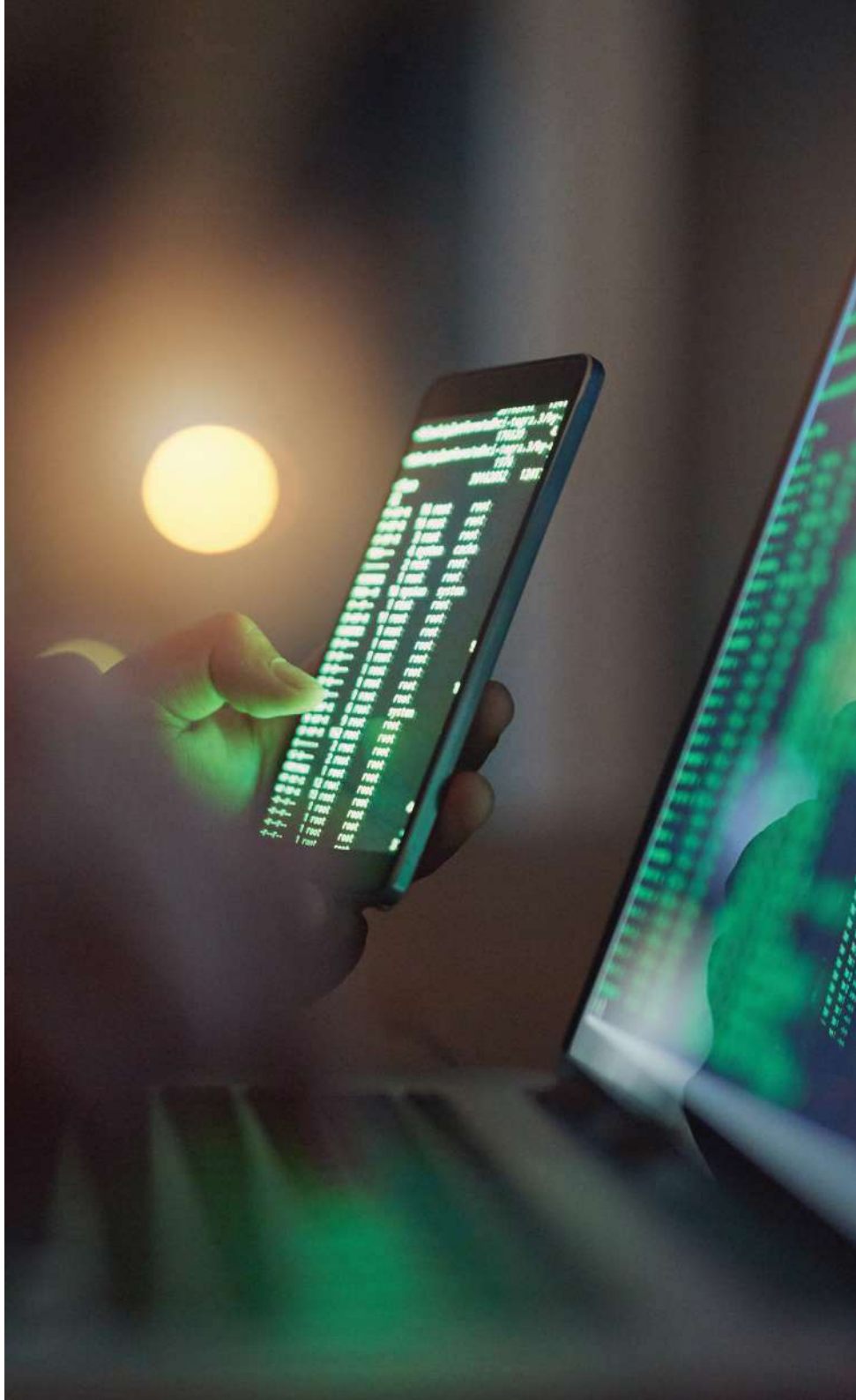
The data of European citizens is protected, even when in the systems of business outside of the EU. It contains 99 Articles within 11 Chapters.

How is GDPR related to Privacy by Design?

Privacy by design is an old concept in the field of systems engineering, and its meaning is obvious. It is a well-known term within both legal and technical communities.

It is very important to state that privacy by design is part of the GDPR, even that the principles of PbD are not detailed in the GDPR. Privacy by Design has always been part of data protection law. The key change with the GDPR is that it is now a legal requirement. Each principle of PbD is related to specific articles within the GDPR.

The GDPR and Privacy by Design introduce new challenges for organizations; new requirements and obligations for legal and compliance functions and more emphasis on organizational accountability towards data protection. Moreover, Articles 42 and 43 of GDPR promote certification as a good tool to show compliance with the requirements.



What does GDPR states for Privacy by Design?

In its article 25, paragraphs 1 and 2, GDPR requires:

1. Taking into account the state of the art (Principle 4: Full functionality - positive sum, not zero-sum), the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons **(Principle 7: Respect user privacy)** posed by the processing, the controller shall, both at the time of the determination **(Principle 1: Proactive not reactive; preventative not remedial)** of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards **(Principle 3: Privacy embedded into design)** into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. (Principle 6: Visibility and transparency)
2. The controller shall implement appropriate technical and organizational measures for ensuring that, by default, (**Principle 2: Privacy as the default setting)** only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. **(Principle 5: End-to-end security - Lifecycle protection)**

For making it simple, the GDPR requires:

1. **Data protection by design:** data controllers must put technical and organizational measures such as pseudonymisation in place – to minimize personal data processing;
2. **Data protection by default:** data controllers must only process data that are necessary, to an extent that is necessary, and must only store data as long as necessary.

The GDPR now makes this design mandatory rather than advisory, so being prepared is highly important

MSECB

www.msecb.com