General Data Protection Regulation: threat or opportunity? (1/28/18)

The General Data Protection Regulation (GDPR) has been in force for over a month. Many organisations are still in the process of putting all the necessary organisational procedures in place and looking for cost-effective solutions to implement all GDPR requirements. Among other things the GDPR requires that a data manager should adopt appropriate technical and organisational procedures, but a detailed description is not provided. In practice, organisations are facing substantially different requirements — acceptable to some entities but unreasonable, expensive and unnecessary for others. How do we check that our security procedures are adequate and demands our business partners make are not excessive?

What is secure personal data processing?

Although the GDPR does not change the personal data protection principles, it gives more rights to the data subject and accordingly imposes new obligations on data processors and managers, which could mainly involve new organisational procedures and technical solutions, in particular relating to physical security in the working environment and IT systems adaptation.

The security standards (including ISO) that are used in various industries imply that personal data should be processed in a secure way according to the following three principles:

1. Confidentiality (e.g. encryption, anonymisation);
2. Availability (e.g. restricted access to data); and
3. Integrity (e.g. data input and movement supervision, data continuity and accuracy).

It’s important to realise there is more to personal data processing than using data actively (gathering, registering, recording, disclosing, sharing etc). Processing includes deletion as well as storing data on paper in a cupboard or electronically on a server even if that data is not used in a long time. So these principles are important when it comes to sharing personal data with third parties and tidying up the working and electronic environment in your organisation.

Reasonable organisational procedures and technical solutions

The GDPR says these procedures should be put in place at a reasonable cost to ensure they are appropriate and necessary by assessing each case on its own merits. This means that each organisation should find a solution that is appropriate and economically sound. For example, a situation where the data manager as a larger organisation requires unreasonable IT security procedures from the data processor is not acceptable. At the same time, data managers that transfer large amounts or special categories of data to data processors can make demands that are more extensive than those applicable to small-scale processing.

Steps to take

To understand what security procedures should be put in place, your organisation should begin by answering the following questions:

1. What kind of personal data is processed (e.g. first name, surname, personal ID number, residence

address, IP address, email, and nationality)?
2. What is the data processed for (e.g. sending commercial messages/news/offers, transferring money, selling goods, or providing services)?
3. Who receives the data (e.g. a human resources officer, insurance companies, banks, or business partners)?

Having gathered this information, your organisation should evaluate risks associated with personal data processing, for example, by assessing whether and how you ensure access control, how vulnerable your information system that processes personal data is to hacking, whether your working environment is secure enough to prevent unauthorised access to your premises and personal data etc.

You are free to choose security procedures that will cover the risks you have identified.

Suggestions for future steps

You haven't missed a thing

If you haven't yet started or completed your implementation procedures, it's no big deal since organisations can still make the necessary preparations. If in doubt you can always consult a certified data protection officer, who will provide a personal data processing compliance assessment in line with the GDPR.

Advise first!

The National Data Office has repeatedly announced they will apply the *Advise First!* principle. In other words, they undertake to begin by explaining the new GDPR requirements to organisations. And the GDPR permits the regulator to give a reprimand instead of a fine if the latter is likely to inflict an unreasonable burden on the organisation concerned.

A benefit for your organisation

Although some organisations feel the measures required by the GDPR are burdensome and unnecessary, we still suggest viewing the GDPR as an incentive to tidy up your working environment, internal processes and contractual obligations, because revising your documents and processes means an opportunity to improve and facilitate your business operations (as well as cutting costs).