CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

ARE YOU READY FOR THE NEW DATA PROTECTION RULES?

10 questions to help prepare your organization for the General Data Protection Regulation (GDPR)

TO STAY UPDATED, VISIT WWW.CNPD.LU

The General Data Protection Regulation will establish a single European data protection regime, replacing the directive from 1995 and Luxembourg's law from 2002.

Are you aware of the new and strengthened rights of individuals?

Besides existing rights (e.g. right to access, right to rectification), data controllers will have to prepare for new and extended rights of data subjects such as the extended right to erasure ("right to be forgotten") and the right to data portability. Do you have procedures in place to transfer personal data to individuals or to other organizations electronically and in a "structured machine-readable" format?

Do you know that you have to comply with the GDPR by May 25th, 2018?

While existing national data protection laws will continue to apply until that date, time has come to assess the impact the new legal framework will have on your organization. It is important to allocate enough time and resources to ensure that compliance with the GDPR is achieved before that deadline.

Is your organization affected?

The GDPR will not only apply to organizations established in the EU (data controllers and processors), but also to organizations established outside the EU offering goods or services to, or monitor the behaviour of, individuals in the EU. This means that the GDPR will also affect organizations previously not subject to the data protection regime.

Are you aware of your personal data processing activities?

A first step towards effective data protection in your organization consists in identifying and documenting all personal data flows (e.g. employee data, customer data). What is the legal ground for any existing data processing and what is its purpose? Where does the data come from and who are the recipients? Where is the data stored and who can access it? The GDPR will require controllers and processors to maintain detailed records of processing activities.

Are you developing or using data protection friendly products and services?

Organizations have to adopt a Data protection by design approach. This means that they should take into account privacy and security measures when designing, implementing or using new systems and services. Data Protection Impact Assessments (DPIA) will be required for projects where privacy risks are high. In some cases, you will be required to consult the CNPD prior to processing. It is also good practice to keep yourself informed about privacy enhancing technologies that might be relevant in the context of the organization's data processing activities.

Will you have to appoint a Data Protection Officer?

The GDPR requires that public authorities or companies whose processing activities include the regular and systematic monitoring of individuals appoint a Data Protection Officer (DPO). The DPO has to be involved in all matters that concern the protection of personal data. You should assess now whether you should appoint a DPO. Do you have people within your organization that could be put in charge of data protection issues? If not, do you need to hire somebody?

Do you have appropriate security measures in place?

The GDPR requires you to regularly document and to review the security measures you have in place. Can you ensure a level of security appropriate to the risks of the data processing? Are you able to restore the personal data in case of an incident? How do you guarantee the confidentiality and integrity of sensitive data?

Do you know that you must report a personal data breach to the CNPD within 72 hours after its detection?

This obligation only holds if the data breach is likely to pose a risk to the rights and freedoms of the data subjects. If this risk is high, then the controller also has to communicate the breach to affected data subjects.

If you are a data processor, you should make sure that you have the right procedures in place to inform the controller of data breaches.

Do you know that there will be tougher penalties for organizations that breach the Regulation?

The CNPD, Luxembourg's data protection authority, will be able to impose fines of 20 million euros or up to 4% of the total worldwide annual turnover (whichever is the greater), where controllers are responsible for serious breaches of the Regulation.

Will you have to review and update (if necessary) existing contracts with data processors?

Data processing that is carried out by a processor on behalf of a controller has to be governed by a contract or another legal act that binds the processor to the controller. The GDPR further specifies the content of the contract or other legal act.

Are you a data controller or a processor?

DATA CONTROLLER: determines the purposes and means of the processing of personal data

DATA PROCESSOR: processes personal data on behalf of a data controller

Commission nationale pour la protection des données
1, avenue du Rock'n'Roll
L-4361 Esch-sur-Alzette
Tél.: (+352) 26 10 60-1
Fax: (+352) 26 10 60-29
E-mail: info@cnpd.lu