European Commission

Digital Single Market

Commission strengthens trust and gives a boost to the data economy

New data protection rules in European union institutions and bodies

By 25 May 2018, the rules on data protection applicable to personal data processed by the European Union Institutions must be aligned with the higher standards set out by the General Protection Regulation (GDPR).

The European institutions and its bodies handle, for instance, the data of its staff (medical records amongst others), of visitors, persons which receive EU funding. They will benefit from new rights and stronger data protection rules, in line with the latest Data Protection rules.

KEY CHANGES

RIGHTS OF DATA SUBJECTS

i) Transparency

European Union institutions and bodies will have to use clear and plain language and make information easy to access. For instance, privacy statements will have to be made in a more visible and concise way.

ii) Right to be forgotten

- A person can request the erasure of their personal data if it is no longer needed, if they object to or withdraw consent for the processing of their data, or if their data was unlawfully processed .
- This right is not absolute, but needs to be balanced against other rights on a case-by-case basis.
- European Union institutions and bodies will have to inform any other persons/organisations processing this personal data (e.g. search engines), if a person has raised objections.

iii) Right to data portability

A person can transfer their personal data from one data controller to another. Where technically possible, the controller must directly transfer the personal data itself.

CONSENT

Union institutions and bodies will have to ask for consent, in clear and plain language, before processing personal data (i.e. always opt-in). They must ask for separate consent for each type of data processing activity (i.e. no bundled consent).

A person can choose to revoke their consent at any time.

NOTIFYING THE EUROPEAN DATA PROTECTION SUPERVISOR AND THE DATA SUBJECT ABOUT A DATA BREACH

European Union institutions and bodies will have to notify the European Data Protection Supervisor (EDPS) about a data breach as soon as they become aware of it, and no later than 72 hours after the breach.

If the data breach poses a high risk to the rights and freedoms of a person, the European Union institutions and bodies will have to inform them of the breach without undue delay. However, this is not obligatory if the controller has already taken measures to prevent the risk, or if it is too difficult to provide this information.

SIMPLIFICATION AND ADMINISTRATIVE SAVINGS

The new rules will abolish unnecessary bureaucratic requirements such as notification obligations and prior checks. These changes will cut red tape and generate savings for the EU budget.

ADMINISTRATIVE FINES

The European Data Protection Supervisor will have the power to impose administrative fines, if a European Union institution or body violates the data protection rules. Fines will be used a as a mechanism of last resort, if the order to respect data protection rules is not respected.

DATA PROTECTION BY DESIGN AND BY DEFAULT

Data protection by design: Union institutions and bodies will have to take appropriate measures (technical and organisational) to make sure that data protection is part of the data processing operation.

Data protection by default: Only personal data that is necessary for the specific purpose of the data processing should be processed.

DATA PROTECTION IMPACT ASSESSMENT

European Union institutions and bodies will have to carry out a Data Protection Impact Assessment (DPIA) prior to the processing of data, in cases where it could pose a high risk to the rights and freedoms of individuals.

A DPIA describes the data processing operation and its purposes, the risks to the rights and freedoms of individuals, and the concrete measures envisaged to address these risks.