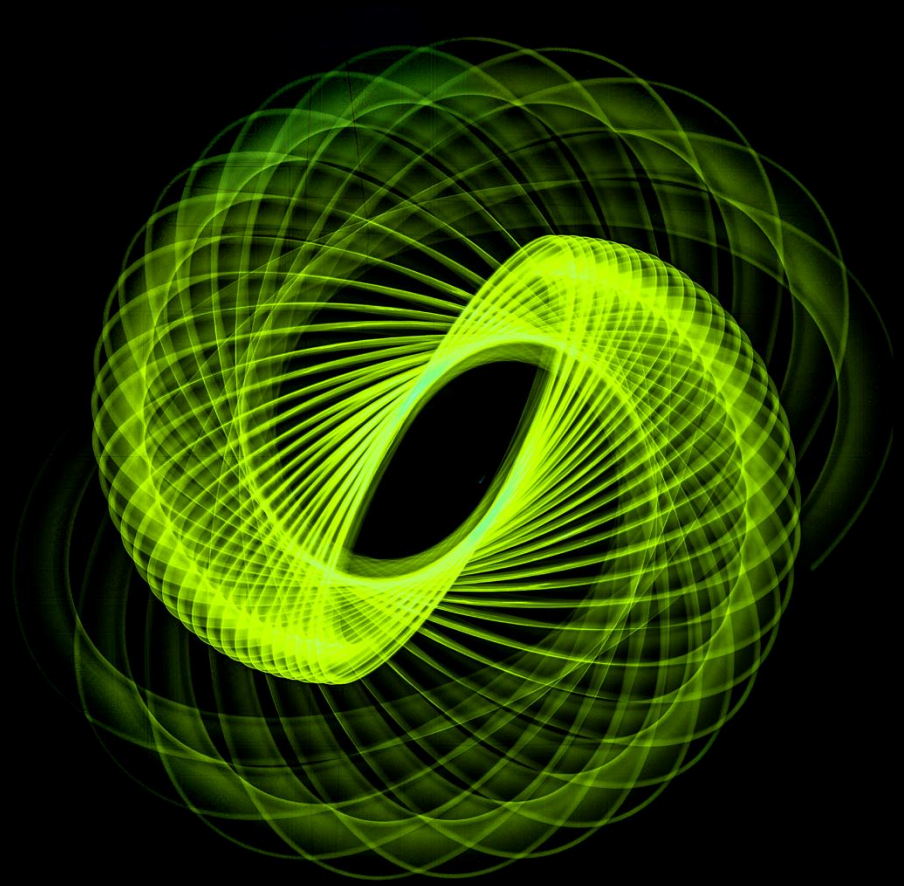
Deloitte.



GDPR compliance in 72 hours: Methodology and applicable IT solutions

Deloitte CIS

October 5, 2018

The General Data Protection Regulation (**GDPR**) is, as of May 25, 2018, the main data protection legal framework in the EU.

GDPR is directly applicable to all EU entities and extraterritorially to non-EU entities that:

- offer goods or services to individuals in the EU and process their personal data;

or

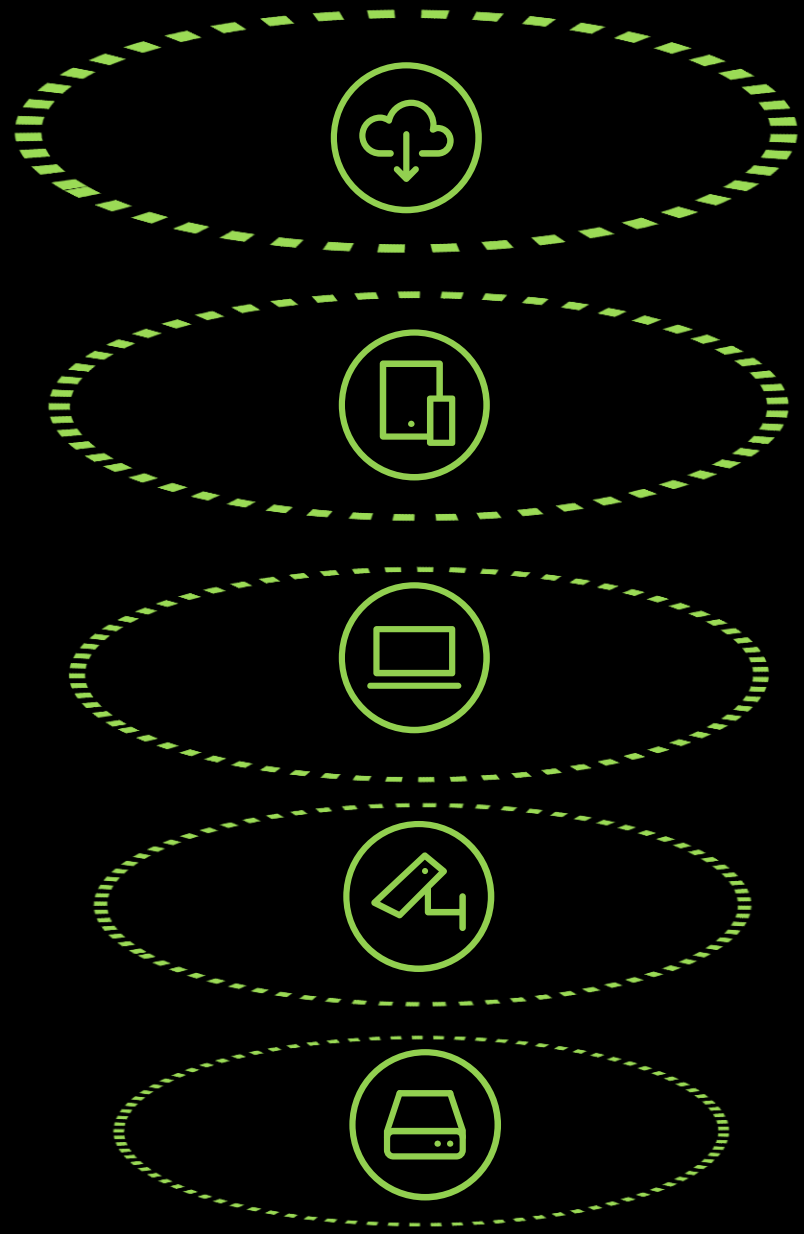
- monitor EU-based individuals' activity in the EU.

One of the core obligations for all businesses is to **ensure a level of security** of personal data by the means of implementing appropriate technical and organizational measures.

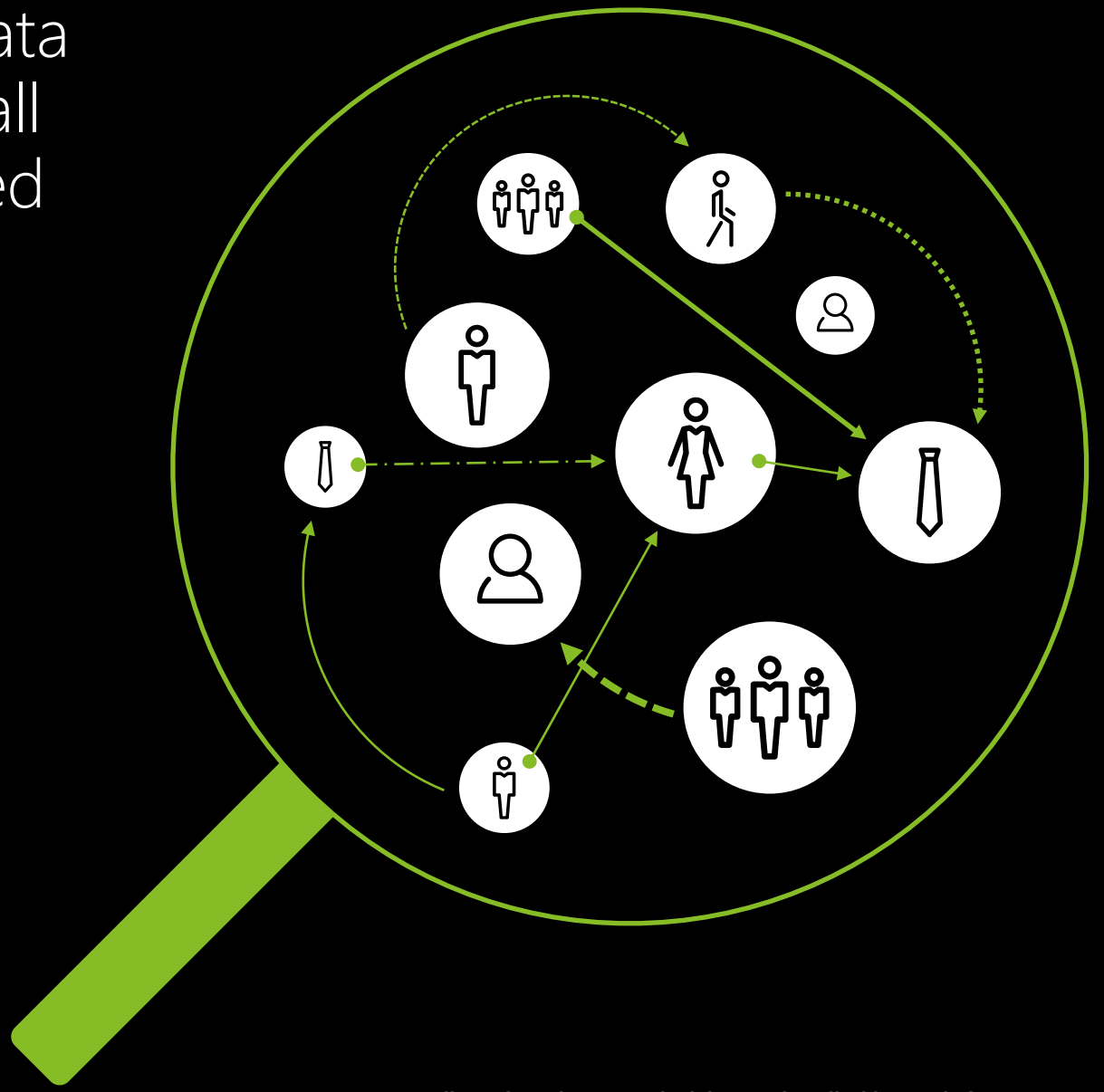
Security of processing is not just a provision of GDPR, it shall be considered within the overall framework for data protection.

GDPR requires companies to:

- record all processing activities;
- control data storage, use, access and transfer;
- ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- detect and investigate data breaches and notify the supervisory authority of a personal data breach within 72 hours.



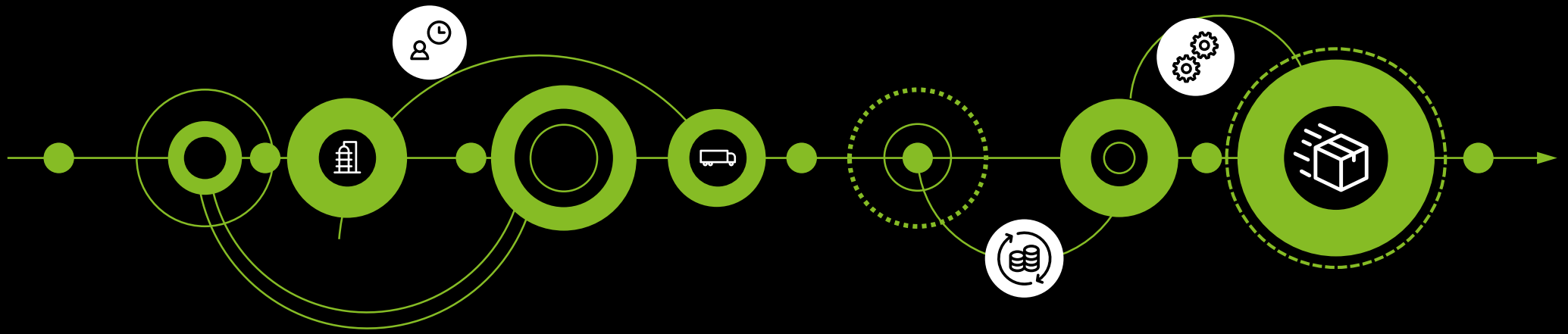
It is essential to perform an initial data processing audit in order to reveal all data flows. Additionally, all processed types of personal data shall be categorized.



The European Union Agency for Network and Information Security (**ENISA**) *inter alia* recommends to implement the following measures:

- allocate control rights inside the company;
- register IT resources;
- document personal data breaches;
- control access and authenticate users;
- identify and track users' actions;
- restrict users from performing actions that could compromise security (such as prohibition of transferring personal data to external devices).

Processed data shall be classified so that data are protected from unauthorized access and unlawful processing.



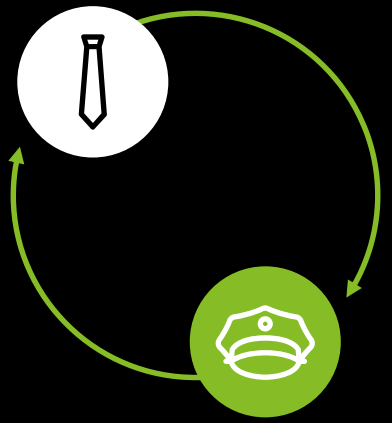
One of the most reliable IT measures could be the use of DLP systems.

DLP system traces the processing and transfer of personal data and allows to control location of data.

With the use of DLP system it is possible to:

- receive notifications of attempts to transfer data to an unauthorized IT system;
- preventively block any attempts of unauthorized transfers.

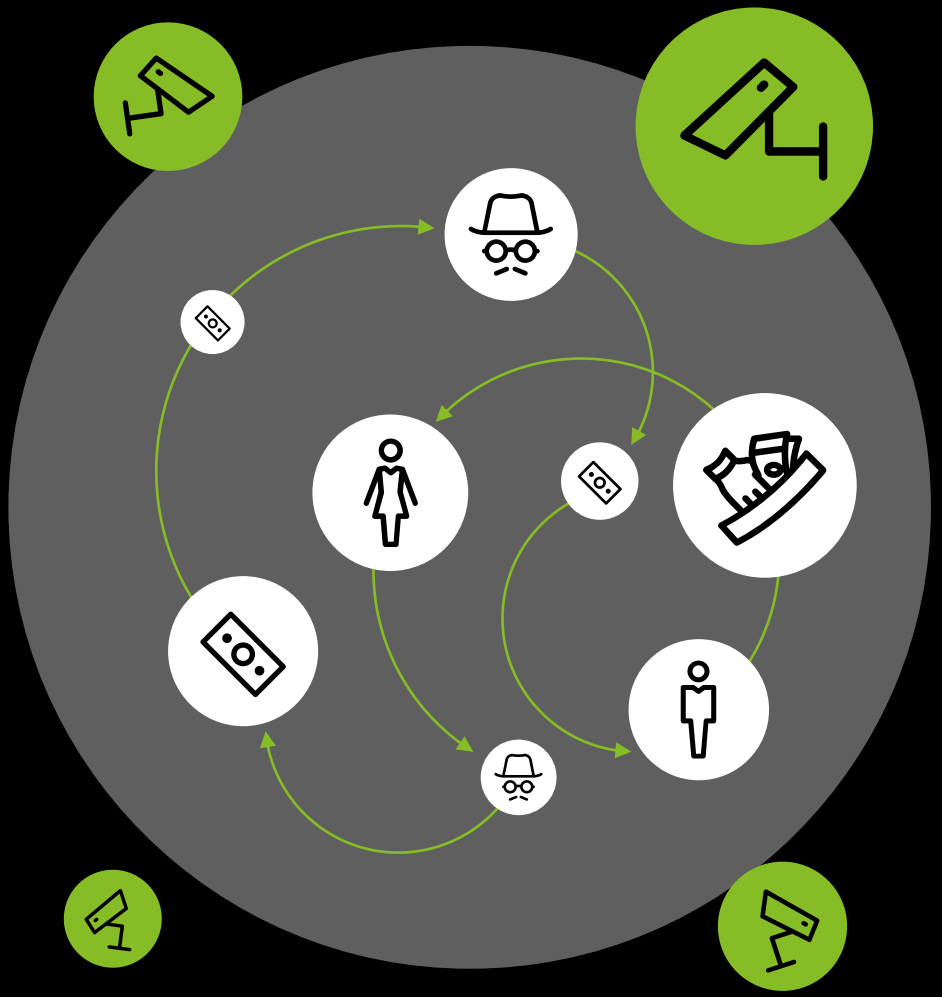
Company shall notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it. Where there is likely a high risk to the rights and freedoms of individuals as the result of a breach, they must also be informed.



DLP system blocks unauthorized personal data processing and notifies DPO. Hence, a data breach could be prevented at the early stage. And the company will obtain relevant information about the data breach.

GDPR provides data subjects with a wide scope of rights, including **right of access** (data subject could obtain confirmation as to whether or not personal data is processed and details of the processing).

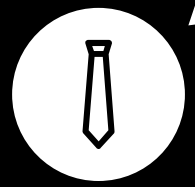
DLP Systems allow to manage data processing and highlight all actions concerning data transfers on an ongoing basis.



Individuals can require data to be erased when there is a problem with the legality of the processing. Additionally individuals can require restriction of data processing.

DLP systems allow to control processing of personal data and erase data or restrict processing when it is required.

Individuals have the right to require their data to be provided in a structured, commonly used and machine readable form so that it may be transferred by the data subject (or even by the controller) to another data controller without hindrance.



DLP systems allow to obtain a copy of up-to-date details of personal data processed by the company.

DLP systems could be both the easiest and the most convenient instrument of GDPR compliance.

Ready-to-use instrument for GDPR compliance

Wide range of measures allowing prevention of data breaches

Specifically designed settings simplify execution of DPO duties

Alexander Tarasenko
Director
FAS
altarasenko@deloitte.ru

Pavel Rykalin
Director
FAS
prykalin@deloitte.ru

Ildar Zverev
Senior manager
Deloitte Legal
ilzverev@deloitte.ru

Natalya Yakovleva
Senior consultant
Deloitte Legal
nyakovleva@deloitte.ru

Deloitte.

deloitte.ru

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 264,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.