JOYN

DATA PROTECTION – IMPACTS OF GDPR IN THE BANKING & FINANCIAL SECTORS

June 2017

APPLICATION OF REGULATION (EU) 2016/679 (GDPR):

25 May 2018

ARTICLE 29 WORKING PARTY GUIDELINES

- DPO
- Data portability
- Lead DPA
- DPIA

DRAFT RECOMMANDATION BELGIAN PRIVACY COMMISSION ON DPIA

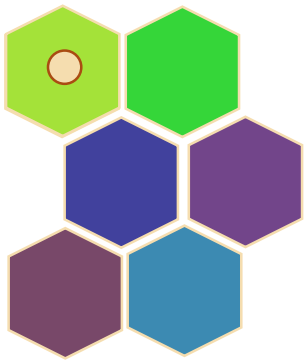
OBJECTIVES OF GDPR

- Increase data subjects' control of their data and boosting digital economy.
- A single set of rules valid across the EU with a lead supervisory authority in case of cross-border processings, limitation of administrative costs (suppression of the processing notification requirements).
- Increased responsibility and accountability for those processing personal data (e.g. notification of data breaches, impact assessment, record of processing, designation of a DPO, etc.).
- Strengthening consent requirement.
- Enhancing data subjects' rights, new right to data portability.
- Increased sanctions.

IMPACTS FOR BANKS, INVESTMENT FIRMS AND INSURERS ("DATA CONTROLLERS") WHEN PROCESSING PERSONAL DATA OF THEIR CLIENTS OR PROSPECTS

JOYN

ACTORS



Data subject

Data controllers

Data protection officer **DPO**

Data processors

Data Protection Authority **DPA**

What is your lead DPA in case your insurance company has several branches in the EU?

As a small bank, should you designate a DPO?

DATA PROTECTION AUTHORITIES: ONE-STOP-SHOP *NEW*

- In case of cross-border processing: designation of a **lead** supervisory authority (DPA).
- Lead DPA = DPA of the controller's *place of central administration* in the EU.
- 'Non-lead DPA' remains active where either: (a) the processor is established in another EU Member State than the controller, (b) data subjects are subtantialy affected by the processing, or (c) a complaint is received locally.

❖ A French insurance company having a Belgian branch processing Belgian client's data and subcontracting the storage of data to a Polish processor.

→Lead DPA = CNIL (French DPA)

→Non-lead DPA = Belgian Privacy Commission and Polish Privacy Commission

DATA PROTECTION OFFICER *NEW*

Designation:

- Mandatory designation of a data protection officer (DPO) in case of processing of customer data in the regular course of business by an insurance company or a bank.
- The DPO may be internal or external and designated for several organisations (e.g. 1 DPO for the bank-controller and its processor), provided that he/she is easily accessible from each establishment to the data subjects, the DPA and within the organisation.
- Expertise requirements: knowledge of data protection law (GDPR and local EU laws) and understanding of the processing operations, IT and data security, knowledge of business sector.

Position of the DPO:

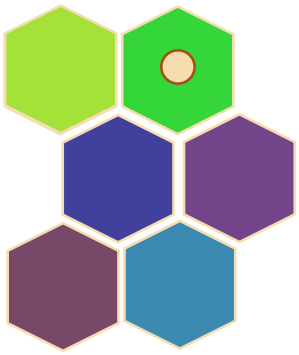
- The DPO must have sufficient resources to carry out his/her tasks (e.g. active support by senior management, sufficient time, continuous training, access to other services e.g. IT department, infrastrucutre, etc.).
- The DPO shall act in an independent manner (no instruction from the controller/processor, no dismissal or penalty for the performance of the tasks, no conflict of interest with possible other tasks and duties e.g. head of HR or IT departments) → could be the compliance officer of a bank.

Tasks of the DPO:

- Monitoring compliance (identification of processing activities, analyse and check the compliance thereof, information, advice and recommandation to the controller or the processor).
- Active role with respect to data protection impact assessment (DPIA).
- No personal liability for non-compliance with DP requirements.

JOYN

BASIC PRINCIPLES



Overview

Lawfulness of the processing

Purpose limitation

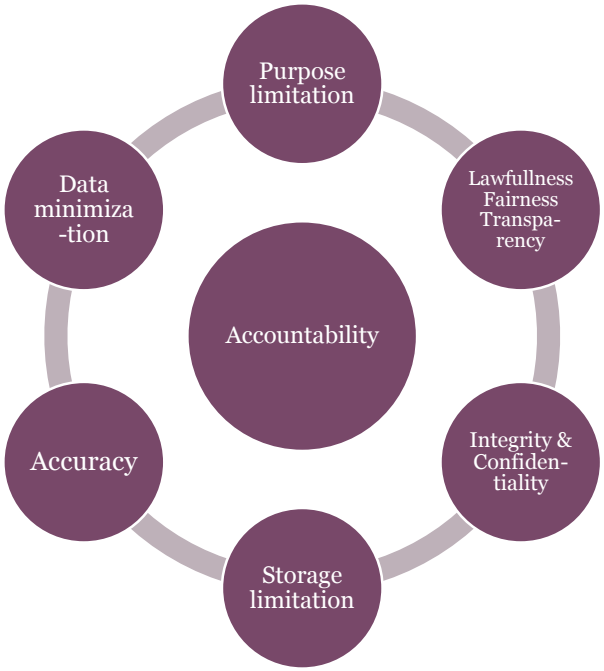
Data minimization

As an investment firm, can you send to your existing clients an offer for additional services as it is provided in the T&Cs?

As a bank, can you force your clients to accept a data localization feature in case they want to open a bank account?

Can you request the previous professions of a client in the frame of a suitability test?

OVERVIEW OF PRINCIPLES APPLICABLE TO ANY PROCESSING



LAWFULNESS OF PROCESSING

Processing is authorized notably where either:

- The processing is necessary to the conclusion or **performance of the contract** (e.g. e-mail address to send updates of the portfolio).
- The processing is necessary for compliance with a **legal obligation** (e.g. AML checks, Mifid/AssurMiFid suitability profiling, solvency profiling for mortgage and consumers credits).
- The processing is necessary for the purposes of the **legitimate interests** of controller (e.g. fraud prevention, security of IT network).
- The data subject has given his/her **consent** to one or more specific purposes (e.g. marketing of new similar banking services).

CONDITIONS OF CONSENT *ENHANCED*

- Consent = any **freely** given, **specific**, **informed** and **unambiguous** indication.
- How? by a statement or by a clear **affirmative action** (e.g. opt-in) → excludes in principle implicit consent, the silence or a pre-ticked box.
- The 'data protection clause' may no longer be part of the T&Cs → it shall be clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

- Each distinct processing requires a **distinct** consent.
- The controller shall be liable to **prove** when and how the data subject consented (e.g. copy of the online consent form in case of online transactions).
- The performance of a contract may **not be conditional** on consent to the processing that is not necessary for the performance of that contract.
  - ❖ A client shall not be obliged to consent to the processing of his/her localization data through a smartphone for the provision of home banking services → risks to invalidate the whole processing.
- The data subject shall be informed to his/her **right to withdraw** the consent at any time. The withdrawal shall be as easy to provide as the consent.
- Where the initial consent is valid, the data may be **further processed** for other purposes than the initial purposes, without a new consent, subject to the purpose limitation principle.

PURPOSE LIMITATION *ENHANCED*

- Data shall be collected for specified, explicit and legitimate purposes.
- Further processing for other purposes than the initial purposes shall be **compatible** with the latter.

  What is compatibility? The controller shall take into account various elements such as the existence of a link between initial and subsequent purposes, the context, the nature of the data, the possible consequences for the data subject, and appropriate garantees (e.g. pseudonymisation).

  In case the subsequent purposes are not compatible with the initial ones, the processing remains acceptable if the data subject has provided his/her consent or if it has a legal basis.

  ❖ T&Cs of a retail bank: "*We process you data in order to provide the financial services requested* [initial purpose] *and to provide information on other services which you may be interested in and to prevent fraud and abuse of the financial system, and to comply with legal obligations* [other purposes]." →compatible and/or legal basis ✓

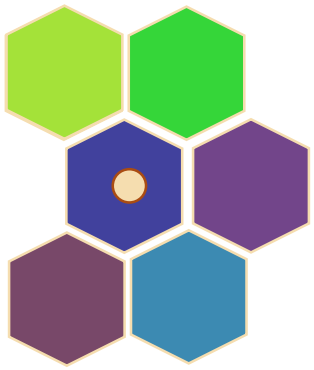
DATA MINIMIZATION *ENHANCED*

The data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

→ implies a storage duration limited to a strict minimum and difficulties to apply with respect to certain obligations of controller (e.g. assessment of creditworthiness and KYC under MiFID 2 requiring ongoing monitoring).

JOYN

ACCOUNTABILITY



Risk-based approach

DPIA

As a small bank, should you carry out a DPIA?

RISK-BASED APPROACH *ENHANCED*

Increase of the level of precautin and attention: the controller shall evaluate the risks to the rights and freedoms of the data subjects on the basis of an objective assessment, by reference to the nature, scope, context and purposes of the processing.

- Risks of discrimination related to the profiling of clients for the granting of consumer credit, of financial loss.

DATA PROTECTION IMPACT ASSESSMENT (DPIA) *NEW*

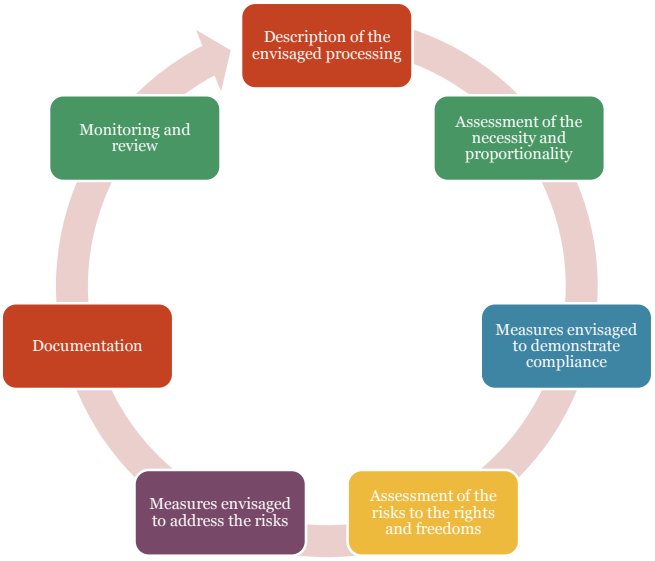
When is a DPIA mandatory?

When the processing is likely to result in high risks for data subjects.

- Banks screening its clients against credit reference database to decide whether to grant or not a loan; an insurance company building marketing profiles based on navigation on its website; monitoring of employees' activities (performance at work, internet use, etc.), automated decision making by AML tool to exclude certain clients from banks

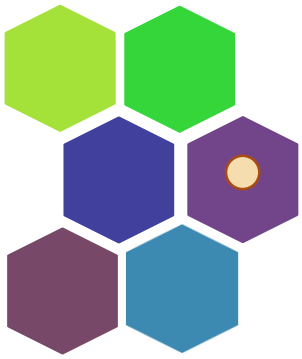
How to carry out a DPIA?

- When? Prior to the processing → as early as practical in the design of the processing / continual update where the processing is dynamic.
- Who? Controller remains eventually responsible to set a DPIA but must seek advice of the DPO, as the case may be with the assistance of the processor.
- WP29 recommends having DPIA published; supervisory authorities shall be consulted in case risks remain unsufficiently managed.
- Iterative methodology:



JOYN

RIGHTS OF THE DATA SUBJECTS



Information requirements

Individual's rights

Profiling

Data portability

Can you refuse to deliver to your client his life-insurance related file to transfer it to his new insurer?

Can you implement an online credit application refusing certain users based on generic criteria?

INFORMATION REQUIREMENTS *ENHANCED*

- **New content to provide:** legal basis for processing the data, data retention periods, transfer of data outside the EU, right to complaint to the Belgian Privacy Commission → privacy notices should be checked.
- Information shall be provided in concise, easy-to-understand and clear langage.

INDIVIDUAL'S RIGHTS

In addition to the right of information, the main rights of indivuals are the rights to (provided for free to the data subjects):

- **access** to their data (*enhanced*): 1 month to address a request of access (vs. 45 days), specific grounds to refuse access (with adequate policies of refusal), additional information to provide to the data subject
- **correct** inaccurate data, **erase** information, **object** to a processing
- prevent automated decision-making and **profiling** (*enhanced*)
- **data portability** (*new*)

PROFILING *ENHANCED*

Principle

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her (e.g.: automated rejection of a credit application online).

Exceptions

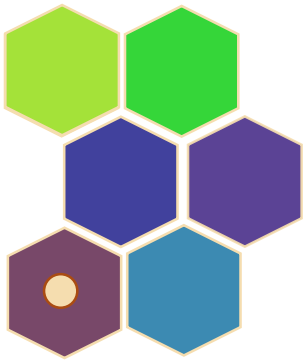
- The decision is necessary for entering into, or performance of, a contract OR is based on the data subject's explicit consent.
  →controller shall however at least implement the right to obtain human intervention, to express his or her point of view and to contest the decision.
- The decision is authorized by EU or Member State law and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests (e.g. fraud detection).

DATA PORTABILITY *NEW*

The data subjects may obtain his/her data, in a structured, commonly used and machine-readable format to allow the transfer thereof to another controller →strengthening of the control over his/her data.

JOYN

SECURITY PROCESSOR TRANSFER



Integrity / confidentiality

Data breaches

Record of processing

Processors

Transfer outside EEA

As a bank, your client database has been accessed without authorization. What should you do?

Can you store your servers in the US, based on your client's consent provided in the data protection clause of the bank's general T&Cs?

INTEGRITY / CONFIDENTIALITY *ENHANCED*

Data shall be processed in a manner that ensures appropriate security of the personal data, including the **pseudonymisation and encryption** of personal data and the ability to **restore** the availability and access to personal data in a timely manner in the event of a physical or technical incident → security measures are more technical.

DATA BREACHES *NEW*

Notification to the DPA

- **When?** In case a breach is likely to result in a risk to the rights and freedoms of natural persons (e.g. identity theft or fraud, financial loss). Notification within 72 hours.
- **Content:** (a) nature of the breach (+approximate number of subjects and records concerned), (b) contact details of DPO, (c) description of the consequences of the breach (d) remediation measures.

Communication to data subjects

- **When?** In case a breach is likely to result in a **high** risk to the rights and freedoms of natural persons. Communication without undue delay.
- **Content:** in clear and plain language the nature of the personal data breach and contain at least the information (b)(c)(d) above.

RECORD OF PROCESSING *NEW*

- The controller and its processor shall each maintain a record of processing activities with various informations (notably the purpose of processing, categories of data and of recipients, third country recipient).
- Exception: entreprise >250 employees (unless processing is likely to result in a risk to the rights and freedom or the processing is not occasional).

PROCESSOR *ENHANCED*

- Obligation to have a contract with the processor with increased obligations on the processor (notably advice and assistance of the controller for individual rights and in case of audit, deletion or return of data to the controller).
- Other obligations: follow controller's documented instructions, restrictions on subcontracting, proof of compliance with GPDR, appointment of DPO as the case arises, enhanced security obligations, record of processing activities, data breach notifications, adequacy decision when transferring data outside EU.

DATA TRANSFER OUTSIDE EEA *ENHANCED*

Rule

Prohibition to transfer data outside the EEA.

Derogations

- Transfers based on **recognized adequacy**:

  Existing rule: EU Commission may recognise that a third country ensures an adequate level of protection to authorize automatically the transfers (e.g. Switzerland).

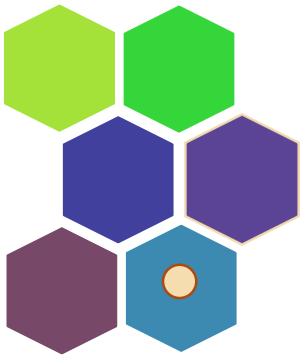
  Extension: GDPR enables adequacy findings also for territories or specified sectors or international orgnanisations other than countries (e.g. EU-US Privacy Shield replacing the Safe harbour → covers only certain sectors for US-based companies).

- Transfers based on **appropriate safeguards** such as Binding Corporate Rules, standard controller clauses, codes of conduct and certification mechanism.

- Transfers based on **other derogations**: explicit consent; the transfer is necessary notably for the performance of the contract or a defence of legal claim; the transfer is made from a public register.

JOYN

CLAIMS SANCTIONS



Remedies

Right to compensation and liability

Administrative sanctions

What could be the sanctions in case your clients' data have been hacked because your IT system was insufficiently secured in light of your organization?

REMEDIES

The data subject shall have the following remedies:

- Right to lodge a complaint with the DPA
- Right to an effective judicial remedy against the DPA (*new*)
- Right to an effective judicial remedy against the controller or processor
- Representation of data subjects to lodge a complaint by: (i) a non-profit organisation through a mandate or (ii) any such organisation acting without mandate (option to be confirmed under local law)

RIGHT TO COMPENSATION AND LIABILITY

- Any person who has suffered material or non-material damage as a result of an infringement shall have the right to receive compensation from the controller or processor for the damage suffered.
- ***New:*** controller, joint controllers and processors are jointly and severally liable towards data subjects to ensure effective compensation.

ADMINISTRATIVE SANCTIONS *NEW*

- DPA shall have the right to impose effective, proportionate and dissuasive administrative fines (in addition to existing criminal sanctions imposed by the criminal judges).
- The amount of the fines shall vary in line with certains criteria, with a maximum 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (in case of infringement to e.g. conditions for consent, data subject's rights, transfer to non EU country).

GDPR – HOW TO GET PREPARED?

GAP ANALYSIS → CHECK:

- Information held (what, where it comes from, existence of transfers, etc.)
- Privacy policies, privacy clauses in T&Cs
- Existing procedures as to individual's rights (erasures, access, correction, objection)
- Consent process (how sought, obtained, recorded)
- Security procedures
- Is DPO required?
- Is DPIA required?
- Identify your Lead DPA

TO DO

- Set up record of processing
- Adapt privacy policies and prepare specific privacy clauses
- Adapt internal procedures to handle enhanced individuals' rights (e.g. right to portability)
- Adapt to enhanced consent process (recording of consent, etc.)
- Adapt security procedures and set up a data breach policy
- Designate a DPO if necessary
- Prepare a DPIA if necessary
- Draft internal privacy process policy involving the various department concerned (IT, HR, compliance, etc.)

JOYN Legal
Ch. de La Hulpe – 181/24 – Terhulpsestwg.
1170 Brussels – Belgium
T : +32 2 738 02 80
F : +32 2 738 02 81
www.joynlegal.be

Déborah Menasse
dmenasse@joynlegal.be

Christophe Steyaert
csteyaert@joynlegal.be