May 2018

STEPS FORWARD IN IMPLEMENTING THE GENERAL DATA PROTECTION REGULATION

(GDPR)

Association des Banques et Banquiers, Luxembourg
The Luxembourg Bankers' Association
Luxemburger Bankenvereinigung

Steps forward in implementing the General Data Protection Regulation ("GDPR"[1])

The Luxembourg Bankers' Association ("ABBL") is the professional organisation representing the majority of banks and other financial intermediaries established in Luxembourg.

Its purpose lies in defending and fostering the professional interests of its members. As such, it acts as the voice of the whole sector on various matters in both national and international organisations.

The ABBL counts amongst its members universal banks, covered bonds issuing banks, public banks, other professionals of the financial sector ("PSF"), financial service providers and ancillary service providers to the financial industry.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

	FOREWORD	**5**
1	**General Considerations/Definitions**	**7**
2	**Expanded Territorial Scope**	**7**
3	**Data Protection core principles under the framework of the Regulation**	**8**
4	**Data retention: Regulation in light of other legal provisions**	**10**
5	**Data subjects' consent**	**18**
5.1	Recap: consent as one out of six criteria to allow for a lawful processing	18
5.2	Shall consent be used as lawful criterion for a processing	18
5.3	In presence of a minor child	21
6	**The Accountability principle and remaining consultation formalities to be accomplished towards the CNPD**	**21**
6.1	Accountability	21
6.2	Remaining obligation of prior consultation towards the CNPD: DPIA	22
6.3	"One-stop shop" and "main establishment"	24
7	**Widening of the scope of the Controller's obligations in view of the new powers conferred upon the data subjects**	**24**
7.1	Provision of information upon collection of data (Transparency requirements)	25
7.2	Access and rectification exerted by the data subject	26
7.3	Restriction and objection	26
7.4	Right to not being subject to Automated decision making and Profiling	27
7.5	Erasure ("right to be forgotten")	27
7.6	Data portability	28
8	**Data Protection Officer (DPO)**	**32**
9	**Data Breach**	**33**
9.1	Scope	33
9.2	Data Breach Notification	33
10	**Data Transfer to Third Countries out of EEA**	**35**
10.1	Appropriate Safeguards	35
10.2	Derogations for specific situations	36
10.3	Invoking "legitimate interests"	36
10.4	Specific situation with regard to the transfer of personal data to the United States	36
11	**Controller/Processor relationship**	**37**
12	**Sanctions**	**37**
13	**HOW MAY CONTROLLERS TAKE EFFECTIVE ACTION TOWARDS THE REGULATION**	**38**
	Appendix I: CONSENT (Drafting efficient consent notices)	**40**
	Appendix II: DATA BREACH NOTIFICATION	**42**
	Appendix III: ACTION PLAN – IN BRIEF	**45**

FOREWORD

The purpose of the following Memorandum consists in briefly recalling the novelties introduced by the Regulation, while suggesting what data controllers/processors may complete to comply with the latter, which will come into force on 25 May 2018 in all EU Member States.

Therefore, **the ABBL hereby emphasises key practical aspects/positions** recently developed by the European Banking Federation ("EBF") with regard to the guidelines of the article 29 Working Party ("Art. 29 WP"), soon to become the European Data Protection Board ("EDPB"). It is important to note that the EBF acts as the voice of the European banking sector, whose pragmatic positions mirror those of the whole European banking industry. The EBF cannot be assimilated to a public authority.

The EDPB core mission will consist in contributing to the consistent application of the Regulation throughout the Union, especially in issuing guidelines, recommendations and statements on many topics. The Luxembourg National Commission for the Protection of Data ("CNPD") regularly refers to the guidelines issued by the Art. 29 WP, constituting the underlying pillar of issues stemming from the Regulation.

Having taken this into consideration, **the CNPD will most certainly always abide/refer to the guidelines issued by the Art. 29 WP**. Members shall hence take such guidelines into due consideration when applying their data protection procedures, as the CNPD may base its controls according to the explanations contained in such guidelines.

In addition, **this memorandum aspires to provide its readers not only with relevant information reflecting the work undertaken by the EBF, but moreover with useful cross border tools/sources to help stakeholders best achieve their obligations towards the Regulation**. To this end, **one may consult the side bar ("*useful tools/information*")** at the end of each point of the memorandum, to get valuable facts/material to implement processes and procedures pertaining thereto.

The employment relationship and its challenges under the Regulation will not be investigated here, as the ABBL issued another practical guide pertaining thereto.

It is to be noted that a **change of paradigm** will occur when the Regulation enters into force, as processing will neither be needed to be notified to the CNPD, nor be authorised by the latter, as is the case with the Act of 2 August 2002 on the protection of individuals with regard to the processing of personal data.

This document has been drawn up for information purposes and does not aim at being exhaustive. It does not constitute legal advice, nor does it attempt to interpret the rule of law. It may nonetheless be regarded as a reference handbook for the setting-up of internal procedures.

Moreover, the content of this document is likely to change depending on the final adoption of the law transposing the GDPR, as well as the clarifications made by the Art.29 WP and the CNPD. It has also been produced given the evolving state of draft law Nr 7184. As a result, the present guidelines may be further updated and supplemented in the future. Finally, one has to bear in mind that other legislations regarding the protection of privacy also apply simultaneously with the GDPR.

These guidelines have been drafted as a result of the active contribution from the members of the "**Data Protection**" working group:

Members

Parul **ABBOTT**	Danske Bank International S.A.
Nathalie **CLOSTER**	ING Luxembourg
Isabelle **COMHAIRE**	Clifford Chance S.C.S.
Philippe **CRABIT**	ING Luxembourg
Michael **HOFMANN**	KPMG Luxembourg, Société Coopérative
Martine **KAYSER**	Banque et Caisse d'Epargne de l'Etat, Luxembourg
Andriana **MARMARA**	UBS EUROPE SE, Luxembourg Branch
Serge **MUNTEN**	Banque Internationale à Luxembourg S.A.
Matthieu **PERBAL**	Credit Suisse (Luxembourg) S.A.
Bieneke **RUSSON**	Société Générale Bank & Trust
Christiane **SCHON**	Banque Internationale à Luxembourg S.A.
Aurélia **SCHWANDER**	Banque Internationale à Luxembourg S.A.
Nathalie **SPRAUER**	Banque Raiffeisen
Christine **THOMAS**	Pictet & Cie (Europe) S.A.
Rute **VENDEIRINHO**	Banque Internationale à Luxembourg S.A.

Secretariat

Catherine **BOURIN**	ABBL
Julien **LEROY**	ABBL

1- General Considerations/Definitions

To start with, it is worth recalling that Directive 95/46/EC on data protection ("Data Protection Directive") was implemented in Luxembourg through the Act of 2002 relating to the protection of individuals in relation to the processing of personal data ("2002 Act"). The 2002 Act, which will no longer apply when the Regulation comes into force, aims at protecting the freedom and fundamental rights of individuals, and notably their private life, in relation to the processing of their personal data. The CNPD is responsible for enforcing these rules in Luxembourg.

Some of the definitions below may prove helpful when dealing with certain provisions of the Regulation, such as for instance:

'Consent' means "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

'Controller', as it is defined in the Regulation, is "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data".

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

One may refer to the relevant examples provided for by the ABBL as to what constitutes personal data within the banking sector.[2]

'Processing' means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

'Processor' means "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".

'Profiling' is to be understood as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

It is worth noting that **most banks are to be considered as controllers by the Regulation, bearing in mind that close ties/enhanced contractual relationships will certainly apply with entities acting as processors** (i.e. service providers acting on behalf of the controller) in the context of outsourcing activities.

2- Expanded Territorial Scope

The 2002 Act governs processing activities by (i) controllers located in Luxembourg and (ii) controllers located outside Luxembourg or the EU, but using means of processing in Luxembourg. **The Regulation modifies this rule**.

Paragraph 2 of Article 3 of the Regulation foresees that the Regulation applies to "the processing of personal data of data subjects who are in the Union by

2 According to a workshop of the ABBL held on 30 May 2017 entitled "Defining what is Personal Data":
See https://www.abbl.lu/topic/general-data-protection-regulation/ (point 2).

a controller or processor not established in the Union, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union or
- the monitoring of their behaviour as far as their behaviour takes place within the European Union."

This means that controllers established in non-EU countries which process data regarding data subjects located in the EU in the context of the provision of goods or services (such as for example offering financial services through a website) will have to comply with the requirements set out in the Regulation. Accordingly, the processing of personal data and the rights of the data subjects pertaining thereto shall be safeguarded in accordance with the Regulation.

The Regulation will also be relevant for members in the context of service providers/processors located outside the EEA, i.e. in "third countries", as the Regulation will apply to such service providers, only if the latter handle/process personal data of natural persons.

According to doctrine,[3] the provisions of the Regulation will apply to entities established in third countries if they have a physical base ("*établissement*")/ server in Europe or if they provide goods-services to data subjects in the EU or monitor the latter's behaviour.

USEFUL INFORMATION

https://cnpd.public.lu/en/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees.html

https://www.privacycommission.be/en/node/19237

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

3 Alain BENSOUSSAN, « Règlement Européen sur la protection des données : textes, commentaires et orientations pratiques », p.66.

3- Data Protection core principles under the framework of the Regulation

The data protection core principles are stated in Article 5 of the Regulation. According to the said Article, personal data must be:

- *"**processed lawfully**, **fairly**, and in a transparent manner in relation to the data subject;*
- ***collected for specified, explicit and legitimate purposes** and not further processed for other purposes incompatible with those purposes;*
- *adequate, relevant and **limited to what is necessary in relation to the purposes** for which data is processed;*
- accurate and, where necessary, kept up to date;
- ***kept** in a form that permits identification of data subjects **for no longer than is necessary for the purposes** for which the personal data is processed, and*
- *processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*

The controller is responsible for, and must demonstrate compliance with, such principles."

TO THE POINT

- *As recalled by the CNPD, controllers, after having inquired on the upcoming Regulation's novelties, shall firstly* ***identify their processing****, that is to say notably:*
  - *determine the categories of data at stake,*
  - *the purposes for which they are being collected,*
  - *the actors which are processing the data (any outsourcing?),*
  - *the flows of data (any transfer in a third country?).*
- Key issue here relies in the **setting up of a Register of processing activities** mainly recalling the aforementioned criteria (see art. 30 of the Regulation).
- It shall not however be forgotten that Art. 30(5) of the Regulation recalls that this obligation shall not apply to entities employing fewer than 250 persons **unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional**, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences.

  The Art. 29 WP recalled on 19 April 2018 in its position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) of the Regulation that the record of processing activities is a very useful means to support an analysis of the implications of any processing whether existing or planned. The record facilitates the factual assessment of the risk of the processing activities performed by a controller or processor on individuals' rights, and the identification and implementation of appropriate security measures to safeguard personal data – both key components of accountability contained in the Regulation.

  Having previously done a data mapping, such **records of processing activities shall hence be the core element for banks to determine the actions which shall be undertaken to comply with the Regulation**, be it for their prospects/ clients, subcontractors and on an internal basis.

  The registry of processing will be key for financial stakeholders to be able to report to **the CNPD, especially in the case of controls** (https://cnpd.public.lu/fr/actualites/national/2017/10/seances-info-GDPR.html, see "*le contrôle de la conformité par la CNPD*") if the controller took the legal necessary steps to comply with the Regulation, given the processing at stake.

  The CNPD provides on its website (see below "GDPR compliance support tools") helpful functionalities/examples of what a registry shall be made of, together with a list of potential processing (in French). It may also be recommended to examine the public Register of processing maintained by the CNPD to gather the core processing within the financial sector.

  Other data protections authorities provide controllers/processors with examples of processing activities (see below).

  As various forms of "records of processing" are available (see below the suggested templates made available by data protection authorities), controllers will be able to set–up their own registry accordingly.

USEFUL TOOLS

https://cst.cnpd.lu/portal/ (GDPR Compliance Support Tool **issued by the CNPD**–see especially parts I and II)

https://cnpd.public.lu/fr/registre/application.html (to make a search within the Public Register)

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/
(see especially "document templates for controllers and for processors")

https://www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement
(see template of Registry developed by the Belgian data protection Commissioner – in French)

https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles
(see notably "*Modèle de registre règlement européen*" and "exemple de fiche de registre CIL"; the latter can be adapted according to the processing realised.

4- Data retention: Regulation in light of other legal provisions

Art. 5.1) b, of the Regulation clearly states that **personal data shall not be further processed in a manner that is incompatible with a clearly defined purpose** (specified, explicit and legitimate).

Besides, Art. 5.1) e, of the Regulation recalls that such personal data shall **be kept** in a form which permits identification of data subjects **for no longer than is necessary for the purposes for which the personal data are processed**.

Hence, once the purpose as defined by the bank/controller is over, such personal data shall, in principle, not be held anymore.

- **HOWEVER**, discretion is not wholly granted to banks, which shall pay due regard to existing legal rules notably emphasised below:

PURPOSE OF PROCESSING	LEGAL FRAMEWORK IN LUXEMBOURG	RETENTION	PROVISIONS FROM OTHER MEMBER STATES and ADDITIONAL COMMENTS
Generally, any communication between banks and their clients (i.e.data subjects)	▪ Art. 189 of the **Commerce Code** (prescription/limitation period).	▪ **10 years prescription/limitation period** for legal actions re. commercial transactions.	
Otherwise, Documents, books of accounts, supporting documents, letters received and copies of letters sent. (Correspondence)	▪ Art. 16 of the **Commerce Code** (profit and loss/annual **accounts**).	▪ **10 years after close of financial year to which they relate.**	
MORE SPECIFICALLY			
Customers' identification details. (**Including beneficial owners'** details)	▪ Art. 3 (6) a, of the **law of 13 February 2018** ("AML Law").	▪ Copy or references of documents, data and information necessary to comply to customer's due diligence: **5 years after end of** business relationship **OR after** end of transaction concluded on an occasional basis (deletion thereafter – without prejudice to longer retention periods prescribed by other laws **or if necessary to implement effective AML/CTF procedures).** ▪ **CSSF/CAA/AED may require to keep those data for** another period of 5 years. ▪ Professionals may (also) retain the data **for** 5 years on top of the initial 5 years period.	

PURPOSE OF PROCESSING	LEGAL FRAMEWORK IN LUXEMBOURG	RETENTION	PROVISIONS FROM OTHER MEMBER STATES and ADDITIONAL COMMENTS
Documents and information re. **Transactions** made by clients. (ONLY for AML purposes)	▪ Art. 3 (6) a, of the **law of 13 February 2018.**	▪ Supporting documents and records of transactions: **5 years after end of business relationship OR** after end of transaction concluded on an occasional basis (deletion thereafter - without prejudice to longer retention periods prescribed by other laws). ▪ **CSSF/CAA/AED may require to keep those data for another period of 5 years.** ▪ Professionals may (also) retain the data **for 5 years on top of the initial 5 years period**.	
Management of **loans/credit facilities**	▪ **Only reference to data law of 2 August 2002** (solvability) in **the law of 23 December 2016** on mortgages. (Nothing more), as transposed in the **Consumers' Code**.	Hence **apply the Commerce Code rule** (as per article 189).	▪ **10 years limitation period** where professionals must be able to prove the execution of their obligations. Legal action prohibited thereafter.
Credit scoring models			*(According to French standards):* ▪ **If loan not granted**: retain **6 months maximum after demand.** See ***CNIL deliberation N°2008-188*** *regarding the assessment of risks when granting loans/credits.*

PURPOSE OF PROCESSING	LEGAL FRAMEWORK IN LUXEMBOURG	RETENTION	PROVISIONS FROM OTHER MEMBER STATES and ADDITIONAL COMMENTS
Payment incidents ▪ Loans repayments. ▪ Credit cards.	▪ **No specific legislative framework** in Luxembourg.		In France, *5 to 7 years registration within a dedicated register:* *"Fichier de remboursement des crédits aux particuliers (introduced by "arrêté" dated 26 October 2010).* ▪ According to the French **"CNIL" deliberation N°2015-105:** Data must be deleted as soon as debtor proceeds to due payment; **15 months** retention otherwise (France). ▪ According to the French **"CNIL" deliberation N°2014-216:** Data deleted as soon as debtor proceeds to due payment; **3 years** retention otherwise.
Supporting documents: **Collateral.**	**No specific references within the law of 5 August 2005** on financial collateral arrangements.	Hence **apply the Commerce Code rule** (as per Article 189).	ADDITIONAL COMMENTS ▪ **10 years limitation period** where professionals must be able to prove the execution of their obligations. Legal action prohibited thereafter.

PURPOSE OF PROCESSING	LEGAL FRAMEWORK IN LUXEMBOURG	RETENTION	PROVISIONS FROM OTHER MEMBER STATES and ADDITIONAL COMMENTS
Follow-up of financial instruments activity (**MiFID** related). *(Note that the current MiFID legal framework is being amended by a draft law and a draft regulation!).*	▪ **Art. 37-1 (6)** of the **Law of 5 April 1993** on the financial sector.	*"Credit institutions and investment firms shall arrange for **records to be kept of all services and transactions undertaken by them, in accordance with the period laid down in the Commercial Code**, which shall be sufficient to allow the CSSF to monitor compliance with the requirements under this Law and, in particular, their obligations towards clients or potential clients".*	ADDITIONAL COMMENTS *Meaning that the 10 years limitation period should apply.*
	▪ Art. 61 **of the Grand-Ducal Regulation of 13 July 2007** relating to organisational requirements and rules of conduct in the financial sector.	*"Credit institutions and investment firms must retain **all the records required under Article 37-1(6)** of the amended law of 5 April 1993 on the financial sector for a period of **at least five years**".*	*GD Regulation referring to the aforementioned law (Art. 37-1 (6) reckons for record of transactions to be kept for **at least 5 years**.*
	▪ Art. 28 (2) of the **Law of 13 July 2007 on markets in financial instruments.**	*"Credit institutions and investment firms must ensure that the relevant **data relating to all transactions in financial instruments concluded by them**, whether on own account or on behalf of clients, are **at the disposal of the CSSF for at least five years**".*	ADDITIONAL COMMENTS ▪ *Confirms the aforementioned rule "at the CSSF disposal for **at least 5 years**".*
Follow-up of financial instruments activity (**MiFID** related).	▪ Art. 31 of the **Law of 13 July 2007.** *(Note that draft Law N°7157 on market in financial instruments will repeal the law of 13 July).*	The CSSF may demand the communication of **existing telephone and data traffic records**.	▪ **Telephone records** hence to be *at the CSSF disposal for **at least 5 years.*** (Given Art. 28 (2) above). *10 years limitation period*. (In case of legal action undertaken by client). *(Draft Law N°7157 yet recalls that telephone records shall be kept for 5 years and up to 7 years if required by the CSSF).*

PURPOSE OF PROCESSING	LEGAL FRAMEWORK IN LUXEMBOURG	RETENTION	PROVISIONS FROM OTHER MEMBER STATES and ADDITIONAL COMMENTS
	▪ Art. 9 (2) of **EU Regulation N°648/2012 on OTC derivatives**, central counterparties and trade repositories.	"Counterparties shall keep a record of any **derivative contract** they have concluded and any modification for ***at least five years following the termination of the contract***.	*Keep at least 5 years after end of contract.*
	▪ Art. 29 (1) and (2) of **EU Regulation N°648/2012 on OTC derivatives** (…)	"A **CCP** shall maintain, for ***a period of at least 10 years***, **all the records on the services and activity provided** so as to enable the competent authority to monitor the CCP's compliance with this Regulation". "A **CCP** shall maintain, for a period **of at least 10 years following the termination of a contract, all information on all contracts it has processed**".	Rules aimed at central counterparties. ▪ Re. France, see **CNIL simplified norm NS-041** on financial instruments (N°97-066). (bearing in mind the **10 years retention period after end of transaction** by reference to art. L123-22 of the French Commerce Code).
Insiders' lists	▪ Art. 18 (5) of **EU Regulation N°596/2014 on market abuse.**	▪ **Issuers** or any person acting on their behalf or on their account **shall *retain the insider list for a period of at least five years after it is drawn up or updated.***	
Market abuses	▪ Art. 17 of **EU Regulation N°596/2014 on market abuse.**	▪ "**The issuer** shall post and maintain on its website for a period of at **least five years**, **all inside information it is required to disclose publicly**".	
	▪ Art. 28 of **EU Regulation N°596/2014 on market abuse.** No other references within the law of 23 December 2016 on market abuses.	▪ "**Personal data** shall be retained for a **maximum period of five years**" (within the framework of market abuses).	▪ According to the French **"CNIL" deliberation N°2009-359:** (*"Caisse d'Epargne"*): *(Electronic system aimed at detecting market abuses: suspicious transactions lists are **searchable for 45 days to be then archived for three years** by the internal control of the entity).*

- **Re. criminal matters**, the public prosecution lapses according to the crime at stake (i.e. contravention/offence/crime). The delays **vary from one to 10 years**, starting from when the crime has been effected.
- **As to how data shall be deleted after retention, the Regulation remains silent**, bearing in mind that a plain English interpretation of deletion implies **destruction**. This may however be quite challenging in the era of digitalisation. As recollected by the British information Commissioner's office (the "ICO"), there is a significant difference between deleting information irretrievably, archiving it in a structured, retrievable manner or retaining it as random data in an un-emptied electronic wastebasket.
- Members may wish to refer to a guidance released by the ICO (see below "Deleting personal data") putting on strong emphasis on the concept of **putting information "beyond use"**, that is to say not actually deleting the data but making sure that controllers notably **commits to permanent deletion of the information if, or when, this becomes possible**.

  More specifically, the ICO utters that it will be satisfied that information has been put beyond use provided that controllers:
  - Are not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
  - Do not give any other organisation access to the personal data;
  - Surround the personal data with appropriate technical and organisational security, and
  - Commit to permanent deletion of the information if, or when, this becomes possible.

Members though, should be abiding by the principles of privacy by design and by default set out by the Regulation, that is to say notably implement appropriate technical and organisational measures to protect the rights of data subjects, such as for instance the right to erasure (or right to be forgotten).

Consequently, one must be able to clearly demonstrate how the deletion process is being undertaken, and as the case may be, describe and document the difficulties encountered in any process of deletion.

- The Art. 29 WP[4] recalls that the storage period (or criteria to determine it) should be phrased in a way that allows the data subject to assess, on the basis of his or her own situation, **what the retention period will be for specific data/purposes. It is not sufficient for the data controller to generically state that "personal data will be kept as long as necessary for the legitimate purposes of the processing"**.

  In this regard, in the financial sector, companies must often hold personal data for various reasons and purposes. These include multiple legal and regulatory compliance purposes. This hence leads to firms holding many types of personal data for a varying amount of time.

  Accordingly, the drafting a retention schedule within the transparency notices aimed at clients/data subjects shall be appropriate and drafted in broad/general terms with a view to be understood by clients/data subjects.

  Hence, banks should be entitled to a more flexible approach and allow more general descriptions, given Articles 13 (2) a and 14 (2) b of the Regulation.
- The CNPD, in its leaflet "your data protection obligations" (see below) underlines that "**AT THE END OF THE RETENTION PERIOD, DATA MUST BE DELETED OR ANONYMISED**".

  This implies a real choice that the controller will be free to choose what it foresees to do after the expiration of the retention period.

  One may wish to refer to opinion 05/2014 on anonymisation techniques of the Art. 29 WP[5] to get some insights on how such techniques should be implemented.

4 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615250 (Guidelines on Transparency, WP 260, p.33-34)

5 http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.html

The Art. 29 WP stresses that anonymisation techniques can provide privacy guarantees, **but only if their application is engineered appropriately** – which means that the prerequisites (context) and the objective(s) of the anonymisation process must be clearly set out in order to achieve the targeted anonymisation level. In other words, there shall be no coming back on retrieving personal data when the latter have been anonymised.

- **Bear in mind** that controllers shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 (of the Regulation) to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.
- One may also refer to the discussion paper issued by the Digital Banking and FinTech Innovation Cluster of the ABBL on the impact of the GDPR on Big Data and Data Analytics, especially in its point 2 regarding "the definition of techniques to remove personal data".
- **CONCLUSION:** IN THE PRESENCE OF CONFLICTING LAWS, ONE SHALL **OPT FOR THE LONGEST RETENTION PERIOD, GIVEN THE PROCESSING AT STAKE**.

To the extent that Luxembourg professionals deal with a great number of foreign clients, any solution concerning the archiving **time limits must take account of the fact that a given dispute might be governed by legislation other than Luxembourg legislation**.

However, it will be noted that, in the accounting field, the periods for which documents must be kept in the different European States vary, **ranging from five to ten years**.

Thus, by archiving documents for ten years in accordance with Luxembourg law, professionals should not in principle encounter any problem, at least in their relations with clients who reside in Member States of the European Union.

A safety margin should also be added to the statutory time limit of ten years, inasmuch as the **prescription period laid down in Article 189 of the Commercial Code may be interrupted or suspended**.

USEFUL TOOLS

- See also the document of the ABBL entitled "Archiving of documents by financial sector professionals".
- **CNPD information will be found under:**

  https://cnpd.public.lu/fr/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees/Un-renforcement-des-droits-des-individus.html

  https://cnpd.public.lu/en/publications/brochures.html (see p. 3, PROPORTIONATE STORAGE DURATION)
- *"Limiter la conservation des données"* (see https://www.cnil.fr/fr/limiter-la-conservation-des-donnees only French version available)
- *Retaining personal data* (see: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/)
- *Deleting personal data* according to the UK Data protection Act: https://icosearch.ico.org.uk/s/search.html?query=deleting+personal+data+&collection=ico-meta&profile=_default

5- Data subjects' consent [6]

5.1- Recap: consent as one out of six criteria to allow for a lawful processing

It shall be borne in mind that **consent is only one out of six criteria** which allow for a processing to be lawful.

Members shall **use the consent criteria only when strictly necessary for a specific processing at stake**, as the data subject may be able to withdraw his/her consent at any time.[7]

The controller must ensure that the data subject can withdraw his/her consent as easily as it was given beforehand, at any given time.

According to Article 6 of the Regulation, controllers may well use the following lawful criteria to process personal data:

- processing is **necessary for the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is **necessary for compliance with a legal obligation** to which the controller is subject;
- **processing is necessary for the performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller;
- **processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person.

6 See Article 7 of the Regulation.

7 See Art. 7 (3) of the Regulation.

5.2- Shall consent be used as lawful criterion for a processing

According to the Regulation, a **controller bears the burden of proof that the consent is free, specific, informed and unambiguous**. As consequences, the pre-formulated written request for consent by customers (which may also be electronic) must be presented in a manner that is clearly distinguishable, in an intelligible and easily accessible form, using clear and plain language. Therefore, silence or inactivity does not constitute consent. Additionally, the data subject will have the right to withdraw his/her consent at any time.

The Art. 29 WP adopted on 28 November 2017 **guidelines on Consent** (WP 259[8]). The guidelines recall the core elements of consent under the Regulation, which is threefold:

- It must firstly be **freely given**, hence implying a real choice resting upon the data subject, without a clear imbalance of power between the parties.

  Any consent given, which is not necessary for the performance of a contract/service is considered "highly undesirable", leading **controllers to carefully assess any "tying" or "bundling" situations**.

  Data subjects shall indeed be free to choose the processing's purpose they agree to (granularity), rather than consent to a bundle of processing.

  *"Tying" the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of that contract or service, is considered highly undesirable. If consent is given in this situation, **it is presumed to be not freely given** (recital 43 of the Regulation)".*

8 See http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615239

- The consent must accordingly be **specific**. To comply with this element, the controller must apply:
  - Purpose specification as a **safeguard against "function creep"** (that is to say go beyond the processing's purpose determined at first by the controller).
  - **Granularity in consent** requests, and
  - Clear separation of information related to obtaining consent for data processing activities from information about other matters.
- Finally, consent must be **informed**, entailing financial stakeholders (controllers/processors) to abide to transparency rules (**see below**).

TO THE POINT

- **Art. 29 WP reckons that "the two lawful basis for the lawful processing of personal data, i.e. consent and contract, cannot be merged and blurred", therefore confirming the strength of the lawful processing criteria of "performance of a contract" as the case may be**.

  As emphasised above and given Article 6 of the Regulation, **consent is only one out of six criteria**, which allow for a processing to be lawful.
- One shall note that the consent hereby emphasised is solely to be understood within the meaning of the Regulation, given that it may be used in other specific laws and be considered differently.
- It will be crucial for the financial services providers to be transparent while collecting customer data when the processing is based on consent.

  Additionally, it will be important to **keep a proper and comprehensive record of the given consent** since there might be cases where proof of consent will have to be presented on request to the relevant Data Protection Authority (DPA).

  The clear difference between the current Data Protection Act of 2 August 2002 and the Regulation relies in the fact that the Regulation expressly requires that the data subject makes a **clear statement or affirmative action to give his/her consent**.
- More practically, the Regulation **does not allow controllers to offer pre-ticked boxes or opt-out constructions** that require an intervention from the data subject to prevent agreement (for example 'opt-out boxes').
- **Blanket acceptance** of general terms and conditions **cannot be seen as a clear affirmative action to consent** to the use of personal.
- It is important to note that Recital 47 of the Regulation states that the processing of **personal data for direct marketing purposes may be regarded as carried out for a legitimate interest**.

However, such provision shall not be used/confused with **marketing effected through electronic mail**, as enshrined in **Art. 11 of the Act of the Act of 30 May 2005**[9] laying down specific provisions for the protection of persons with regard to the processing of personal data in the electronic communications sector (and transposing European Directive 2002/58/EC, soon to be replaced by the E-Privacy Regulation).

- The aforementioned Article 11 (2) on **prior consent exemption** recalls that "(…) where a supplier obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, **that supplier may use those electronic contact details for direct marketing of its own similar products or services provided that customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message where the customer has not initially refused such use**.

  Within the ambit of the 30 May 2005 Act, i.e. electronic communications, controllers will be able to effect marketing towards clients' standard financial products (current accounts/savings accounts) without a prior consent, as long as there is an opt-out **option** conferred upon those clients pertaining to such "standard products".

  If controllers wish to do such e-marketing re. specific/complex categories of product, not directly linked to the core sale of financial product/service made at first by the financial provider, then the **opt-in option will apply**, meaning that controllers will indeed need to get the data subject prior consent to proceed to such marketing.

- **The EBF pinpoints that data subjects shall be prevented from "consent fatigue"**, thus, one shall try to avoid overburdening data subjects with too much information on too many occasions by nudging them too often. An appropriate level of granularity needs to be found that does not lead the data subject to be nudged and bothered constantly, as it risks causing them to disengage from data protection issues. Besides, the Art. 29 WP recalls, in its latest guidelines on consent under the Regulation adopted on 10 April 2018 with regard to the "unambiguous indication of wishes" (see point 3.4), that "**in the digital context**, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of **click fatigue**: when encountered too many times, the actual warning effect of consent mechanisms is diminishing".

- The EBF also strongly highlights that tools, techniques and mechanisms constituting appropriate measures to obtain consent from the data subjects are constantly evolving. Accordingly, it is important **to take a technology-neutral approach and let data controllers to best assess the most efficient way to inform consumer and obtain consent**.

9 "The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) **or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.**"

USEFUL TOOLS

- https://cnpd.public.lu/fr/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees/Un-renforcement-des-droits-des-individus.html
- ***SEE APPENDIX I for drafting efficient consent notices*** (contains valuable information/template of clauses to be adapted to specific processing).
- **See "Privacy notices under the GDPR" to draft comprehensive notices/ clauses**:

  https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/
- **See "GDPR Consent guidance"**

  https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/gdpr-consent-guidance/

  https://www.cnil.fr/fr/modele/mention/formulaire-de-collecte-de-donnees-personnelles

5.3- In presence of a minor child [10]

With regard to the consent of a child aged below 16 years pertaining to the offer of information society services, the processing will be **lawful only if the holder of the parental responsibility over the child gave his/her consent**.

Otherwise, it is to be noted that Member States may fix the threshold to an age below 16, but not below 13, which comes relevant in the context of banks making use of the **freedom to provide services**.

10 See Art.8 of the Regulation.

6- The Accountability principle and remaining consultation formalities to be accomplished towards the CNPD

6.1- Accountability

As emphasised in the foreword, the Regulation introduces **a change of paradigm** whereby processing will neither be needed to be notified to the CNPD, nor be authorised by the latter, as is the case with the 2 August 2002 Data Protection Act.

Accordingly, processors will not be required to proceed to the ex-ante notification of their processing to the CNPD, in addition to not being bound to ask for the CNPD's prior authorisation re. certain categories of processing.

The new principle enshrined in the Regulation also consists in reponsibilising controllers and make them abide to the concept of *"privacy by design and Privacy by default"* as set out in Article 25 of the Regulation.

Privacy by design means that each new service or business process that makes use of personal data must take the protection of such data into consideration. A controller needs to be able to show that it has **adequate security in place and that compliance is monitored**. In practice this means that the persons in charge of the data processing must take privacy into account during the whole life cycle of the system or process development. Privacy by design, different to privacy by default promotes techniques such as **anonymisation** (removing personally identifiable information where it is not needed), **pseudonymisation** (replacing personally identifiable material with artificial identifiers), and **encryption** (encoding messages so only those authorized can read it) to protect personal data.

The concept of "privacy by default" simply means that the strictest privacy settings automatically apply once a customer acquires a new product or service. In other words, no manual change to the privacy settings should be required on the part of the data subject. There is also a temporary element to this principle, as personal information must by default only be kept for the amount of time necessary to provide the product or service.

- Currently, as set out in Article 12 of the law of 2 August 2002, the controller shall make a prior notification of the processing undertaken to the CNPD, exceptions applying as the case may be. **This would not be required any more** under the Regulation as controllers would have to prove to the CNPD that they put their best efforts into **setting up adequate processes and organisational requirements right from the start to safeguards the fundamental rights of data subjects**.
- The CNPD especially recalls this specific point in its preparatory guidelines.[11]

USEFUL INFORMATION

https://cnpd.public.lu/en/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees/responsabilite-accrue-des-responsables-du-traitement.html

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

https://www.cnil.fr/fr/comment-se-preparer-au-reglement-europeen-sur-la-protection-des-donnees

11 See point 6 of the Guidelines.

6.2. Remaining obligation of prior consultation towards the CNPD: DPIA

The controllers shall **consult** the CNPD prior to any processing if **a data protection impact assessment (DPIA)** under Article 35 of the Regulation is at stake. Controllers shall effect a DPIA especially when the processing is likely to result in high risks to the rights and freedoms of natural persons concerned (such as for instance automated processing involving the evaluation of one's personal criteria or profiling).

The controllers will hence be required to put in place effective procedures and mechanisms that focus on the most high-risk operations.

The Art. 29 WP emphasises in its guidelines on DPIA (see below WP 248 rev.01) that nine criteria should be considered in the assessment of processing likely to result in high risks:

- Evaluation or **scoring**, including profiling and predicting, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements" (recitals 71 and 91). Examples of this could include a financial institution that screens its customers against a credit reference database or against an anti-money laundering and counter-terrorist financing (AML/CTF) or fraud database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website.
- **Automated-decision making** with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person".
- Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or "a systematic monitoring of a publicly accessible area".

- **Sensitive data** or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 of the Regulation (for example information about individuals' political opinions), as well as personal data relating to criminal convictions.
- Data processed on a **large scale**: the Regulation does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends to consider a few factors such as the number of data subjects concerned, the volume of data and/or the range of different data items being processed, the duration/permanence of the data processing activity, the geographical extent of the processing activity.
- Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.
- Data concerning vulnerable data subjects.
- **Innovative use or applying new technological** or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc…
- When the processing in itself "prevents data subjects from exercising a right or using a service or a contract".

- **The CNPD** pinpoints in its preparatory guidelines that controllers shall gather all the documentation necessary to prove that they indeed complied with the Regulation's obligation to perform DPIA, which could endanger the fundamental rights of the data subjects.[12]

12 See point 5 of the CNPD guidelines.

USEFUL TOOL/INFORMATION

- **CNIL free Software** to make a DPIA ("logiciel pour realiser son analyse d'impact sur la protection des données":
  https://www.cnil.fr/fr/rgpd-un-logiciel-pour-realiser-son-analyse-dimpact-sur-la-protection-des-donnees-pia
  https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil
- See **dedicated presentation of the CNPD (FR) entitled**: "*les analyses d'impact sur la protection des données*":
  https://cnpd.public.lu/fr/actualites/national/2017/10/seances-info-GDPR.html
- See also *"Nouveautés sur le PIA: guides, outils, PIAF, étude de cas":*
  https://www.cnil.fr/fr/nouveautes-sur-le-pia-guides-outil-piaf-etude-de-cas
- Guidelines Art. 29 WP on data protection impact assessment:
  http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360
- See also the **guidelines** of the UK Information Commissioner's office "conducting privacy impact assessments code of practice" and overall information on DPIA:
  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

6.3- "One-stop shop" and "main establishment"

'**Main establishment**' as defined in Article 4 of the Regulation can be described as the place of the **controller's central administration** in the Union, *unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions shall be considered as the main establishment*.

As regards **a processor** *with establishments in more than one Member State, the place of its central administration in the Union, and, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under the Regulation*;

The Regulation hereby establishes a "**one-stop-shop**" meaning that the companies will only have to **deal with one single supervisory authority** ("DPA"), rather than 28 (see Article 56 of the Regulation re. "*the competence of the lead supervisory authority*"). Where a data controller is established in more than one EU Member State, **the DPA of the main establishment of the data controller will act as the lead authority** for the business' cross-border processing.

It is worth noting that each DPA will have jurisdiction over complaints and possible violations of the Regulation. Article 78 of the Regulation (entitled "*Right to a judicial remedy against a supervisory authority*") gives each natural or legal person the right to an effective judicial remedy against legally binding decisions of a supervisory authority.

- While the "one-stop shop" regime presents advantages for multi-established corporate structures such as fostering the consistency of decision making for the "principal controller" towards its single "lead supervisory authority", it may potentially entail the risk that several data protection authorities claim competence over the data processing activities of such structures.
- Controllers established in several Member States (for ex. a bank with subsidiaries or branches in Luxembourg and headquarters abroad) shall **proceed to a factual assessment of the main place of establishment, which** will eventually determine where the core decisions for the data processing activities will have to be referred to the lead authority.
- Controllers will need to establish proper governance and internal procedures to be able to interact with foreign DPAs as the case may be and raise employee's awareness pertaining thereto.

7- Widening of the scope of the Controller's obligations in view of the new powers conferred upon the data subjects

The 2002 Act already obligated controllers to provide data subjects with specific information when a processing was occurring, on top of exerting specific powers emanating from data subjects with regard to their own data (right of access, right to object, etc [13]…).

The Regulation widens the scope of information to be handled to the data subjects when processing their data together with granting them specific rights to be exerted at their own discretion.

13 See Articles 26 et seq. of the 2002 Act.

7.1- Provision of information upon collection of data (TRANSPARENCY REQUIREMENTS)

As recalled in **Articles 13 and 14** of the Regulation, the controller must notably provide the following information to the data subject upon collection as follows:

- Identity and contact details of the controller, its representative (if any).
- Contact details of the Data Protection Officer ("DPO", if any).
- **Purposes of the processing** and its **legal basis.**
- **Legitimate interest pursued** by the Controller where the lawfulness of the processing is based on such criterion.
- Recipients of data.
- Whether or not **transfer of personal data to third countries** will occur.
- Any other information to ensure a fair processing, such as retention period, right of access, rectification or erasure, right to withdraw consent at any time when the lawfulness of the processing of the processing is based upon such consent, right to lodge a complaint with the DPA, whether or not an automated decision making (including profiling) exists.

- **The CNPD recalls** that it shall be essential for controllers to **be able to prove** that it provided data subjects with the appropriate information together with allowing the latter to exert their specific rights.
- It is highly recommended for controllers to **pay due attention to their contractual clauses** to comply with all of the information requirements as defined in the Regulation.
- Controllers shall also **set up technical procedures** to allow the data subject to effectively exert their rights.
- **The Art. 29 WP released guidelines on transparency**[14] on 24 January 2018.

These guidelines mirror the Regulation's requirements with regard notably to the **information to be provided** by controllers to data subjects (see Articles 13-14) on a **fair basis**, in addition to them being able to **exert their rights in an easy way**.

In short, the information to be delivered must be clear, concise, intelligible and transparent while controllers shall also be able to **explain to data subjects the consequences** of the processing.

One may note that **exceptions** to transparency do apply, depending on whether the data controller has or not obtained the data directly from data subjects (*see p. 25 onwards*).

USEFUL TOOL

- REFER TO APPENDIX I of this document to get helpful tips on taking into consideration "transparency matters" when drafting privacy clauses.
- See "**privacy notices under the GDPR**": https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/

14 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615250

7.2- Access and rectification exerted by the data subject

In the same vein as the provision of information to the data subject when collecting his/her data, the controller must also **on request provide information** to the latter ("*droit d'accès*"),[15] such as:

- Purposes of the processing;
- Categories of data concerned;
- Recipients to whom the data are disclosed;
- Storage period (or criteria to determine it);
- Right of rectification, erasure, restriction or objection;
- Right to lodge a complaint with the DPA;
- Communication of undergoing processing and their source;
- Significance and envisaged consequences of processing in case of automated decision making including profiling.

As per Article 16 of the Regulation, the controller must without undue delay proceed to the rectification of inaccurate personal data and completion of incomplete personal data.

7.3- Restriction and objection

Restriction

In case the data subject exerts his/her right to restriction of processing[16], the controller must **not process the personal data anymore, unless** the data subject gives his/her consent.[17]

15 See for instance Article 15 of the Regulation.

16 For instance when the accuracy of the data is defaulting, unlawful or if the controller no longer needs the data for the purposes of processing and the data subject requires them to exert a legal claim.

17 Public interest, protection of rights of a person, defence of a legal claim.

If the data subject objects the processing when the controller actually based the lawfulness of its processing on "legitimate interests" grounds, it must demonstrate that its legitimate interests take precedence over the rights of the data subject.

This exercise may be difficult to prove by the controller, as its compelling legitimate grounds for processing must at no cost contravene the core rights and freedoms of the data subject.

Objection

Data subject may object the processing if the data are being used for **marketing purposes, including profiling**. In such case, **the data shall no longer be processed for such purposes**.

- Controllers may **try to adopt the highest security measures with regard to the data processed to safeguard the fundamental rights** of the data subjects. Encryption, minimisation, anonymisation, data protection loss, pseudonymisation and other technical measures shall be applied to help not to contravene fundamental rights.[18]
- One shall pay specific attention to **the right to object given to the data subject in combination with a processing based solely for the purposes of the legitimate interests** pursued by the controller. Indeed, the data subject has the right to object to this single lawful criterion of processing just on "**grounds relating to his/her particular situation**" (see Art. 21, 1 of the Regulation) without further information. The controller shall hence try to find additional lawful criteria to proceed to the processing.

18 Kindly refer to the ABBL FAQs on the GDPR : http://www.abbl.lu/topic/general-data-protection-regulation/

- Controllers benefit only from a few derogations whereby they could oppose the right of restriction or objection. Besides, the **controller shall explicitly bring to the attention of the data subject**, clearly and separately from any other information, the data subject's right to object.
- **The CNPD hence advises controllers not only to consider their contractual clauses, but also to organise their in house processes** to manage the data subjects' claims with regard to their rights, as enshrined in the Regulation.[19]

7.4- Right to not being subject to Automated decision making and Profiling

This right applies if a decision is based **solely** on automated processing **and** produces **legal effect** towards the data subject (*particularly relevant in a banking context*).

A data subject cannot claim this right if:

(i) s/he gave its **explicit consent to the automated decision making.**

(ii) it is necessary for entering into or the **performance of a contract** between the data subject and the controller.

If (i) or (ii) apply, the controller shall make sure that the data subject's rights and freedoms are safeguarded, "*at least the right to obtain human intervention on the part of the controller*", for the data subject to express his/her point of view and contest the decision.

(iii) Decision taking is "***authorised by the EU or by a Member State law*** *to which the controller is subject*" (bearing in mind safeguarding the data subject's rights and freedoms).

- **Worth noting that the data subject may challenge a bank's automated decision making/profiling just by claiming a right of human intervention in the process.**
- **The EBF strongly emphasises that financial stakeholders shall be able to apply automated individual decision-making and profiling <u>notably in being compliant with existing legal and supervisory requirements</u> such as those enshrined in the anti-money laundering/MiFID directives.**
- **A right balance shall hence be found between protecting/safeguarding the data subjects' rights as consumers and, on the controller's side, abiding for instance by contractual obligations or legal requirements.**

USEFUL INFORMATION

- See the guidelines of the Art. 29 WP re. automated decision making and profiling:
  http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

7.5- Erasure ("right to be forgotten")

Coming up as a novelty among other ones, the right of being forgotten exerted by the data subject must be undertaken by the processor, which must erase accordingly the personal data gathered when:

- Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- Data subject withdraws his/her consent on which the processing is based, in the case where no other legal grounds remains;

19 See points 4 and 6 of the CNPD guidelines.

- Data subject objects to the processing of personal data and there are no overriding legitimate grounds for the processing, in the case where no other legal grounds remains;
- Data have been unlawfully processed;
- Data have to be erased for compliance with a legal obligation.

The data controller may not assent to the erasure if (notably) necessary for the compliance with a legal obligation requiring processing by EU or Member State law.

7.6- Data portability

Data portability is also a new right that will allow the data subjects to move their personal data from one service provider to another.

Under Article 20(1) of the Regulation, individuals whose personal data are being processed electronically and in a 'structured and commonly used format' are given the right to obtain a copy of that data for further use, *provided that the processing of personal data is* ***based either on consent or on a contract***. Article 20 (2) of the Regulation further provides for the right for individuals to transmit their personal data from one provider to another.

The CNPD provided the ABBL with its comments about data portability (standards and formats),[20] which will be usefully referred to in this section.

Bringing such flexibility to consumers will inevitably lead to increased administration and cost for data controllers.

- Controllers may review their procedures for dealing with requests for data, ensuring that **an efficient process is in place that allows individuals to obtain their data electronically. They may also work on establishing standardized processes to facilitate the transfer of data to other service providers**, including a method of removing any confidential or commercially sensitive information from requested data.

20 Following a workshop organised by the ABBL on 16 June 2017 on the Regulation and the topic of data portability.

The Art. 29 WP released revised guidelines on the right to data portability on 5 April 2017 (the guidelines). The latter were duly analysed by the EBF, focusing on core banking issues raised by stakeholders, that is to say:

(i) **Responsibility** of the controller in the processing handled directly by the data subject;
(ii) **Limitation of the scope of the right of data portability (raw data);**
(iii) **Right of access is not to be confused with the right to data portability;**
(iv) **How to provide the portable data to the data subject/controller;**
(v) **Security matters/time limit.**

(i) Responsibility of the controller in the processing handled directly by the data subject:

The guideline recalls that **data portability is a right of the data** subject to receive a subset of the personal data processed by a data controller, and to store those data for further personal use on a private device without necessarily transmitting the data to another data controller.

As the "sending" data controller cannot prevent adverse effects on any third parties involved in the context of the data portability, the EBF supports the approach adopted by the guidelines recalling that **data controllers answering data portability requests are not responsible for the processing handled by the data subject or by another company receiving personal data**.

(ii)/(iii) Limitation of the scope of the right of data portability/to be distinguished from right of access.

The Regulation clearly emphasises[21] that, to be within the scope of the right to data portability, data must be "**personal data** concerning him/her, **which he or she has provided to a data controller**".

21 See Article 20 (1) of the Regulation.

As recalled by the Art. 29 WP in its guidelines on the right to data portability, inferred data and derived data are created by the data controller on the basis of the data "provided by the data subject". For example, the outcome of an assessment regarding the health of a user or the profile created in the context of risk management and financial regulations (e.g. to assign a credit score or comply with anti-money laundering rules) cannot in themselves be considered as "provided by" the data subject.

Even though such data may be part of a profile kept by a data controller and are inferred or derived from the analysis of data provided by the data subject (through his/her actions for example), these data will typically not be considered as "provided by the data subject" and thus will not be within scope of this new right.

In general, given the policy objectives of the right to data portability, the term "provided by the data subject" must be interpreted broadly, and should exclude "inferred data" and "derived data", which include personal data that are created by a service provider (for example, algorithmic results). A data controller can exclude those inferred data but should include all other personal data provided by the data subject through technical means provided by the controller.

These derived personal data do not fall within the scope of the right to data portability.

The CNPD likewise mentions the guidelines and states that inferred data and derived data are created by the data controller on the basis of the data "*provided by the data subject*".

The CNPD confirmed its statement in October 2017 recalling **that portable data shall not include data created by the controller** (*see slide 12 of the presentation re. data portability*):

https://cnpd.public.lu/fr/actualites/national/2017/10/seances-info-GDPR.html

- This is also the position shared by **the EBF**, recalling that **only the data actively provided by the data subject to the data controller should fall in the scope of right to data portability**.

  The EBF hence endorse the guidelines when the latter states that **inferred data and derived data created by the data controlle**r on the basis of the data "*provided by the data subject*" **shall typically not be considered as "provided by the data subject" and thus not fall within the scope of the new data portability right**.

  The guidelines adds "*for example, the outcome of an assessment regarding the health of a user or the profile created in the context of risk management and financial regulations (e.g. to assign a credit score or comply with anti-money laundering rules) cannot in themselves be considered as "provided by" the data subject. Even though such data may be part of a profile kept by a data controller and are inferred or derived from the analysis of data provided by the data subject, these data will typically not be considered as "provided by the data subject*".

- In short, the EBF believes that an **obvious distinction exists between "raw data" provided for by the client, and "managed/derived data"** which have gone through further processing undertaken by banks acting as controllers.

  Those derived data are those that have undergone further processing, such as verification, internal processing, cybersecurity checks, analysis, etc. **Data that results from the processing of the controller should, by no means be considered as 'raw data' provided by the data subject**. These should belong to the companies that create an **additional level of value based on their know-how**.

  Raw data received by bankers are being enhanced, mostly according to the whole banking and financial legislative framework controllers have to abide to and requiring them to guarantee a higher quality of data; therefore,

such legal processes create an additional layer of value, which cannot be considered as the raw data provided by the data subject to the controller according to the wording of the Regulation and the guidelines.

Besides, passing on inferred/derived data to other EU and non-EU controllers will definitely unfairly benefit them, hence be detrimental to the controller, which enhanced the data.

- **The right of access differs from the right to portability**, as responding to different purposes. Both rights shall not be confused and mixed up, as "it could give the feeling that a wider range of data is communicated with the 'right to data portability' compared to those obtained by exercising 'the right of access' **when to the contrary the right of data portability covers a more limited amount of information"**, according to the EBF.

(iv) How to provide the portable data to the data subject/controller?

The CNPD states that there is no obligation set out in the Regulation to use a standard format, as to how personal data shall be extracted to serve the purpose of data portability. Nonetheless, data subjects shall be delivered with their personal data in a commonly used and machine-readable format, as required by the Regulation.

The EBF too, when commenting upon the Art. 29 WP guidelines, usually tends to promote the concept of "**technology neutrality**" (for instance re. consent matters). Briefly speaking, it means that tools, techniques and mechanisms aiming at implementing certain features/requirements of the Regulation are diverse and constantly evolving.

Accordingly, such technology neutrality should allow controllers themselves to best assess the way they intend to transmit the portable data at stake.

The guidelines recall that controllers shall not hinder the transmission of portable data made to the data subject. If the controller is to transmit data to another controller, such transmission should be exerted **if technically feasible**, meaning that it should not create an obligation for controllers to adopt processing systems, which are technically compatible.

The Art. 29 WP proposes for controllers to envisage **2 options**:

- a direct transmission of the overall dataset of portable data (or several extracts of parts of the global dataset) or
- an automated tool that allows extraction of relevant data.

To achieve such purposes, **controllers might use** for example, **secured messaging, an SFTP server, a secured WebAPI or a WebPortal**. Where no formats are in common use for a given industry or in a given context, **controllers should provide personal data using commonly used open formats (e.g. XML, JSON, CSV) along with useful metadata** at the best possible level of granularity, while maintaining a high level of abstraction.

The Art. 29 WP pinpoints that "*given the wide range of potential data types that could be processed by a data controller,* ***the Regulation does not impose specific recommendations on the format of the personal data to be provided. The most appropriate format will differ across sectors and adequate formats may already exist****, and should always be chosen to achieve the purpose of being interpretable and affording the data subject with a large degree of data portability. As such, formats that are subject to costly licensing constraints would not be considered an adequate approach.*"

(v) Security matters/time limit

- Ensuring **Data security simply refers to** the principle enshrined in the Regulation recapping that appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.[22]
- With regard to the **time limit imposed to answer a portability request**, the guidelines refers to the Regulation requiring that controllers provide "information on action taken" to the data subject **"without undue delay" and in any event "within one month of receipt of the request"**.[23] This one-month period can be extended to a maximum of three months for complex cases, provided that the data subject has been informed about the reasons for such delay within one month of the original request.
- To finish with, it is worth noting that the guidelines did not clarify whether data controllers, which still hold personal data of data subjects, are obligated to comply with a request of data portability **in case the relationship with the customer came to an end**.

  The controller must hence carefully consider the retention period of the personal data they hold (*see point 3 above on data retention*), usually complying with legal or regulatory requirements in force, shall they face such demand by a former client.

USEFUL TOOLS

- See "*le nouveau droit à la portabilité des données*" published by the **CNPD**
  https://cnpd.public.lu/fr/actualites/national/2017/10/seances-info-GDPR.html
- Annex "*Frequently Asked Questions*" of the Article 29 WP guidelines on the right to data portability
  http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233
  https://www.cnil.fr/fr/le-droit-la-portabilite-en-questions (only French version available)
- See guide released by the Information Commissioner's office:
  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/
- See information published by the Belgian Commission:
  https://www.privacycommission.be/fr/droit-a-la-portabilite-de-vos-donnees-art-20-rgpd

22 See Art. 5, 1 (f) of the Regulation

23 See Art. 12 (3) of the Regulation

8- Data Protection Officer (DPO) [24]

The Regulation recalls that a DPO shall notably be designated when:

- **the core activities of the controller or processor consist of processing which, by its nature, scope or purposes, requires regular and systematic monitoring of data subjects on a large scale, or**
- the core activities consist of processing on a large scale of special categories of data.

One could try to argue that banks "core activities" do not consist in processing operations which require "regular and systematic monitoring of data subjects on a large scale".

At first sight however, this regular and systematic monitoring of data subjects on a large scale seems to apply to banking institutions. Nevertheless, it shall take into consideration the size and business model of a bank, leaving room and flexibility in the appointment of a DPO. The CNPD pinpoints this analysis and states that DPOs may well be appointed for instance at group level or on a part-time basis. DPOs shall play a prominent and independent role within an organisation and will anyway be the main point of contact for the CNPD in case of potential controls made by the latter.

There are two ways of appointing a DPO according to Paragraph 8 of Article 35. The DPO can either be an employee of the processor or controller or it can carry out the relevant duties under a services contract.

A group of undertakings can appoint a single DPO. While such obligation did not exist before, not appointing a DPO in cases where it is obligatory pursuant to the Regulation will be heavily sanctioned. The ABBL hence highly recommends for a DPO to be appointed within banks.

The powers which will be conferred to a DPO will be **wide**. Indeed, the Regulation will notably:

- permit the DPO to inform and advise the controller or the processor and the employees on their obligations,
- be involved in any questions pertaining to data issues,
- monitor compliance with the Regulation, the Controller/Processor's policies and Member States Data protection provisions,
- Act as a point of contact for the authorities among others.

- The CNPD in its guidelines (*see point 6*) illustrates the "*regular and systematic monitoring of data subjects*" in comparing a bank's obligation to effect an on-going monitoring of its clients' transactions to fight against money laundering and terrorism financing.
- The CNPD further reveals that a DPO, on top of gathering and taking note of the new obligations enshrined in the Regulation:
- **Be up to date** with the content of any new obligations,
- **Shall raise management's awareness on the impact** these new rules will have on the organisation,
- **Carry out the inventory of the processing**(s),
- **Take positive actions of information**,
- **Continuously supervise compliance** with the Regulation.

USEFUL INFORMATION

- https://www.cnil.fr/cnil-direct/question/1257?visiteur=part
- http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360 (Art. 29 WP guidelines on DPO)

24 See Articles 37-39 of the Regulation

9- Data Breach

9.1- Scope

A personal data breach means, according to the Regulation (see Art. 4 – definitions) a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

This hence encompasses breaches that are the result of both accidental and deliberate causes, which shall be recorded by controllers/processors within a registry (**see appendix II below**).

The CNPD released last month "questions and answers" concerning data breach notifications together with a valuable "data breach notification form".[25]

Within 10 steps, controllers are being providers with clear and concise information on how to react in the case of a data breach notification, that is to say:

- a **Confidentiality breach**: in case of **disclosure** or unauthorized or accidental access to personal data;
- an **Availability breach**: in case of accidental or unauthorized **loss/destructio**n of personal data;
- **an Integrity breach**: in case of accidental or unauthorized **modification** of personal data.

The notification itself either to the CNPD or to data subjects will depend on the degree of risk to the rights and freedoms **of natural persons**, according to the breach (es) at stake. All hence lies within the consequences of the breach(es) **towards individuals**.

9.2- Data Breach Notification

"Data Breach Notification" refers to an obligation of controllers to provide information on the data breaches, such as unauthorized access or other data leaks.

▪ Notification to the CNPD

Article 33 of the Regulation obliges **controllers to notify certain breaches to the DPA without undue delay and where feasible within 72 hours of discovery of a breach**. Late notifications will have to be accompanied by a reasoned justification for the delay. The notification includes information on the breach itself, the measures taken to fix it, and possible consequences.

▪ Notification to the data subject

When the personal data breach is likely to result in a **high risk** to the rights and freedoms of natural persons, the controller will in most cases communicate the personal data breach to the data subject without undue delay.

According to Article 34, 3) of the Regulation, exceptions do apply:

"The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

- *the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;*
- *the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;*
- *it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner".*

The reporting should be made in a tight timeframe (i.e. 72 hours) and controllers will need to document what sort of data has been lost and how such loss has been dealt with.

25 See : https://cnpd.public.lu/fr/declarer/violation-de-donnees/violation-donnees-rgpd.html (inFrench)

TO THE POINT

- Controllers shall implement internal **procedure**s to set out steps to be taken in the event of a data breach.
- Kindly note that the Regulation does not provide with a template of a register re. data breaches. One may be interested in **consulting appendix II, point 3**, providing with a template of what could be used to fill this purpose.
- **According to the CNPD** in its valuable set of information relating to data breaches, (see https://cnpd.public.lu/fr/declarer/violation-de-donnees/violation-donnees-rgpd.html (see point 3 of the aforementioned information):

In case of a data breach, COMMUNICATION TO BE MADE TO THE DATA PROTECTION AUTHORITY shall at least:

- Describe the nature of the personal data breach including, where possible, the categories and approximate number of persons affected by the breach and the categories and the approximate number of personal data records concerned;
- Communicate the name and contact details of the DPO or another point of contact where additional information can be obtained;
- Describe the likely consequences of the personal data breach;
- Describe the measures taken or proposed by the controller to remedy the breach of personal data, including, as the case may be, measures to mitigate any negative consequences.

- **According to the CNPD** in its valuable set of information relating to data breaches, (see https://cnpd.public.lu/fr/declarer/violation-de-donnees/violation-donnees-rgpd.html (see point 4 of the aforementioned information):

In case of a data breach, COMMUNICATION TO BE MADE TO THE DATA SUBJECTS shall at least contain:

- The name and contact details of the data protection officer or another point of contact where additional information can be obtained from;
- A description of the likely consequences of the personal data breach;
- Description of the measures taken or proposed by the controller to remedy the breach of personal data, including, where appropriate, measures to mitigate any negative consequences.

- **The EBF in its key messages** to the Art. 29 WP guidelines reckons:
  - Further clarity as to what constitutes a "*reasonable degree of certainty*" for a controller **when being aware of a breach**,
  - Avoid sparkling unnecessary confusion / alarming data subjects in case of a breach and
  - That banks **stick to common and efficient reporting processes** (avoiding duplication). This latest consideration has been provided for by the CNPD.
- According to the accountability principle, banks acting as controllers will have to **determine the criticity of potential data breaches**.

To this end, they may use the "**Recommendations for a methodology of the assessment of severity of personal data breaches**" published by the European Union Agency Network and Information Security" (ENISA):

https://www.enisa.europa.eu/publications/dbn-severity

USEFUL TOOLS

- See **appendix II** for a data breach notification form **published by the CNPD** https://cnpd.public.lu/fr/declarer/violation-de-donnees/violation-donnees-rgpd.html
- See **appendix II, point 3 presenting** a template of what could be used to record data breaches.
- See also for information purposes the guidances issued by the UK Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
- *http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360* (See also Art. 29 WP Guidelines on Personal Data Breach Notification)

10- Data Transfer to Third Countries out of EEA

The Regulation still recalls the principle of an adequacy decision, bearing in mind that **the Commission solely decides** if a third country ensures an adequate level of protection.

The Regulation introduces certain changes with a specific focus on providing "**appropriate safeguards**" for instance through BCR or SCC (among others…) to permit the transfer of data outside the EEA.

10.1- Appropriate Safeguards

"Binding Corporate Rules" ("BCR")

BCR are set out under Article 47 of the Regulation[26] and described as "*personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers (…) of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity*".

According to the said Article, the BCR must be legally binding and apply to and be enforced by every member of the group of undertakings/enterprises engaged in a joint economic activity, including their employees. The BCR shall be approved by the competent DPA in accordance with the consistency mechanism provided in Article 63 of the Regulation. It is also foreseen that the transfer outside the European Economic Area must be approved by the DPA first.

USEFUL TOOLS

- The European Commission recognised a few countries as providing an adequate level of protection: see https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en#dataprotectionincountriesoutsidetheeu
- The rules as enshrined in the Regulation are quite extensive and **one shall make sure that the future BCRs will match the requirements of the Regulation**.
- See the working document of the Art. 29 WP "on binding corporate rules for processors/controllers":
  http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110
  http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109

Standard Contractual Clauses

Another option to provide adequate safeguards for the transfers according to the Regulation is for controllers to use standard contractual clauses approved either by the Commission or by a DPA. The controller could also try to draft its own contractual clauses, **but the latter will firstly require to be authorised by the DPA**.

26 See also definition within Art. 4 (20) of the Regulation.

USEFUL TOOLS

- See the model contracts for the transfer of personal data to third countries issued by the European Commission: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

10.2- Derogations for specific situations [27]

In the absence of an adequacy decision or appropriate safeguards, data exporters may rely on **explicit consent** from the data subjects to move outside the EU, ensuring simultaneously that the concerned data subjects have been sufficiently informed of the risks of transfer.

Apart from the explicit consent of the data subject, the controller may also proceed to the transfer of data to a third country **if necessary for the performance of contract (i) between the DS and the DC** or (ii) **concluded in the interest of the data subject**.

See also: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360 for positions/recommendations/tools of the Art. 29 WP regarding international transfers of personal data.

10.3- Invoking "legitimate interests"

Article 49 of the Regulation introduces a new derogation to transfer data outside the EEA on the grounds of the controller's "compelling legitimate interests". In such case, the transfer may only take place if the transfer is not repetitive, concerns only a number of data subjects, is necessary for compelling legitimate interests and not overridden by the rights and freedoms of the data subject (the controller having also provided suitable safeguards to the data subject).

The controller shall inform the supervisory authority of the transfer in this case as well as the affected data subject.

27 See Art. 49 of the Regulation.

- The CNPD emphasises in its guidelines that the controller shall be able to **document how it framed/managed data transfers outside the EU** (especially being able to show the contractual clauses/BCR which have been used).
- Hence, **strict contractual rules and enhanced pre-contractual information shall be applied** to ensure compliance with the Regulation.

10.4- Specific situation with regard to the transfer of personal data to the United States

The EU-US privacy shield entered into force on 1st August 2016, given that the European Commission adopted on 12 July 2016 its decision pertaining thereto. The EU-US privacy shield permits for personal data to be transferred from the EU to a company located in the United States, provided that the US company processes the data according to a strong set of data protection rules and safeguards.[28]

This new arrangement includes notably (i) strong data protection obligations on companies receiving personal data from the EU (ii) safeguards on U.S. government access to data (iii) effective protection and redress for individuals and (iv) annual joint review to monitor the implementation.

USEFUL TOOLS

- https://www.cnil.fr/fr/modele/mention/mention-dinformation-en-cas-de-transfert-de-donnees-hors-de-lunion-europeenne
- See also the **dedicated "privacy shield" website** where one (i) will be able to know if an entity is part of the "privacy shield participant list" and (ii) to see the purpose of the data collection they are being certified with: https://www.privacyshield.gov/list

28 See http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf (for detailed information).

11- Controller/Processor relationship

Services level agreements managing the obligations between controllers and their processors will need to be adapted according to the stringent requirements of the Regulation (see notably Art. 28 of the Regulation).

Accordingly, it will be essential for controllers/processors to clearly define the scope of their obligations within a contract, that is to say notably:

- Determine the list of processing to be undertaken, including for instance the type of data at stake, the purposes/lawfulness of the processing.
- Set out the precise roles of each contracting parties and their liability in case of breach of contract: e.g. processor to act according to terms defined by the controller/the assistance between the parties in various matters/how transparency and the exercice of rights by data subjects are to be organised.
- Ensure the highest compliance with the data protection by default/design's rules.
- Fix the obligation to create a register to record the processing and one for data breach. In this regard, it is very important that both the controller and the processor agree on a specific timing, whereby the processor will have to inform the controller of a data breach as the case may be, given the tight "reporting obligation" to the data protection authority ("without undue delay and, where feasible, not later than 72 hours after having become aware of the breach").
- Set out how data will be returned to the controller after the end of the contractual relationship.

USEFUL TOOLS

Information provided by the CNPD:

- https://cnpd.public.lu/fr/actualites/national/2016/10/conference-CNPD-SMC-1110.html
- See **the templates** in French and English made available by the French Data protection authority for drafting purposes: https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses

12- Sanctions

As from May 2018, the Regulation contains sanctions which will depend on the breach made by the controller, varying from fines of up to 10 million euros or 2% of the total worldwide annual turnover (if related to provisions/principles such as "by design and by default", non-compliance with processing related obligations or failure to appoint a DPO). Fines may even range up to 20 million euros or 4% of the total worldwide annual turnover of the previous financial year (if breach relates to lawful processing or breach of data subjects' rights).

USEFUL INFORMATION

- **Sanctions shall be duly taken into consideration** and be for instance discussed at the board of directors' level. The managers shall be duly informed so that they take the relevant measures beforehand. Internal trainings specially designed for the board can be organized so that they become fully aware of the consequences of non-compliance with the Regulation.
- See also for your information:
- the guidelines of the Art. 29 WP on the application and setting of administrative fines. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237
- **the presentation of the CNPD** regarding "le contrôle de la conformité" https://cnpd.public.lu/fr/actualites/national/2017/10/seances-info-GDPR.html

13- HOW MAY CONTROLLERS TAKE EFFECTIVE ACTION TOWARDS THE REGULATION

The CNPD gives hints on how controllers shall document their compliance with the Regulation[29], notably in following a "**three steps approach**" encompassing (A) Processing (B) People and (C) Actors.

This constitutes a good summary of the core work controllers needs to undertake to abide to the requirements enshrined in the Regulation and be able to document their business processes and procedures pertaining thereto.

Readers may also wish to refer to the "Action plan" referred to in appendix III below.

▶ PROCESSING

- In order to justify the handling of personal data, stakeholders shall set up a **Register**/Records of processing: SEE TOOLS POINT 2 SUPRA.
- In the presence of **transfer of data to third countries**, controllers shall be able to demonstrate how they applied adequate safeguards toward the data subjects by making use of the options detailed in the Regulation (such as for instance standard contractual clauses, binding corporate rules or the use of specific derogations): SEE POINT 10 ABOVE.
- As the case may be, the **outcome of the data protection impact assessment**: SEE TOOLS POINT 6.2
- Establish a specific **register re. data breach notification**, in case of data breaches: SEE TOOLS POINT 9 ABOVE (and the recent guidelines of the CNPD in this regard).

▶ PEOPLE

- **Forms set out to get the data subjects' consent** (as the case may be) shall be made available.
- Controllers shall be able to **make available all the procedures/processes designed for data subjects to exert their rights**.

▶ ACTORS

- Contracts between the controller and its processor(s) shall be amended according to the Regulation's requirements.
- Retain proof of data subjects' consent if a processing is based on consent.

▶ OTHERS

- Controllers shall put their best efforts in establishing the highest guarantees with regard to implementing data protection by design and by default, that is to say implement appropriate technical and organisational measures notably at the level of information system/technology.

OVERALL USEFUL TOOLS

- GDPR compliance support tool launched by the CNPD https://www.privacycommission.be/fr/th%C3%A8mes-0 (Q & A re. data protection issues from the Belgian data protection commissioner).
- **"Preparing for the General Data Protection Regulation – 12 Steps to take now!"**
  Guide issued by the UK Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- Go to **"Plan en 13 étapes"** (Belgian Data protection Commissioner) https://www.privacycommission.be/fr/reglement-general-sur-la-protection-des-donnees-0

29 See point 7 of the preparatory guidelines to the Regulation of the CNPD "*Documenter la conformité*".

APPENDIX

APPENDIX I
CONSENT (Drafting efficient consent notices)

PART A
"WHAT NOTICES SHALL BE MADE OF"

Readers shall be aware that the CNPD stresses in point the last point (7) of its preparatory guide to the Regulation entitled *"Document compliance"* that controllers shall be able to **prove that data subjects actually gave their consent to a processing**, together with the **templates used** to collect their consent.

- To get the data subject's consent, it is of utmost importance for members to **abide to the transparency rules as set out in Art. 13 and 14** of the Regulation, which exhaustively list the information criteria controllers shall hand on to the data subjects, depending on the situation at hand (either data collected directly from the data subject by the controller, or indirectly).

  The **criteria shall be checked according to the purpose of the processing**, having noted that some of them may not apply as the case may be.
- **Point 3.3.1 of the Art. 29 WP guidelines on Consent depicts in a concise manner the information required to obtain a valid consent**, that is to say:

1 - the controller's identity;
2 - the **purpose** of each of the processing operations for which consent is sought;
3 - what **(type of) data** will be collected and used;
4 - the existence of the **right to withdraw** consent;
5 - **information about the use of the data for decisions based solely on automated processing**, including profiling, in accordance with Article 22 (2) of the Regulation (Mortgages for instance);
6 - if the consent **relates to transfers**, obtain consent about/mention the possible risks of data transfers to third countries in the absence of an adequacy decision and appropriate safeguards.

According to the nature of the consent requested, other criteria enshrined in the aforementioned Articles 13/14 may come handy in the drafting of consent clauses.

PART B
A CONSENT FORM, FOR INSTANCE, COULD BE WORDED AS FOLLOWS:

"In order to (*describe processing and purpose*)….

(*Bank X)* needs to get your consent according to the legal framework pertaining to the protection of personal data, to process your data for such purposes (*be explicit- legal basis involved and legitimate interests as the case may be*).

Only your (*name, surname etc… insert the data which will be collected*) will be collected solely by (*Bank X*) (*otherwise mention the other recipients + transfer issues third countries as the case may be*) and be kept no longer than necessary for the aforementioned processing's purpose (*mention duration of retention/legal requirements/criteria used to determine duration*).

You have a right of access and rectification to your personal data, together with the right to erasure shall you no longer wish for your personal data to be processed by (*Bank X*), (*etc… describe the rights conferred upon the data subjects*).

You may withdraw your consent at any time through (*find one or more procedures to do so and mention what will happen in case of withdrawal*).

(*Should it be the case, indicate if the processed data will be subject to an automated decision making, including profiling + develop on such mechanism): To be able to … (insert purpose), (Bank X) will carry on an automated decision making process (unless commanded by contract or authorised by law)*.

(*Insert reference to the right of the data subject to lodge a complaint with the CNPD*): You may address any claim with regard to (*refer to processing*) to the National Commission for Data Protection (*you may insert contact details of the CNPD*).

- To finish with, create a specific consent layer/part whereby the data subject gives his/her consent.

THE AFOREMENTIONED COMPONENTS MAY USEFULLY BE USED TO REFLECT THE TRANSPARENCY REQUIREMENTS AS REQUIRED BY THE REGULATION:

PART C

In view to comply with the transparency requirements, one may wish to benefit from the Art. 29 WP comments on information requirements set out below:[30]

- **Go to**: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615250

and see schedule entitled "Information that must be provided to a data subject under Article 13 or Article 14", especially the column dedicated to Art. 29 WP comments.

30 See schedule of the guidelines on transparency (WP 260), starting p. 32 onwards.

APPENDIX II
DATA BREACH NOTIFICATION

TEMPLATE PROVIDED BY THE CNPD

Financial stakeholders shall use the data breach notification form provided by the CNPD by clicking on the link below:

To be downloaded from:

https://cnpd.public.lu/fr/declarer/violation-de-donnees/violation-donnees-rgpd.html (also available in English).

Members will also find the relevant information relating to data breach notification (in French language) as provided by the CNPD under:

https://cnpd.public.lu/fr/declarer/violation-de-donnees/violation-donnees-rgpd.html

▸ **Only for illustration purposes**, one may interested in seeing below the template issued by the UK Information Commissionner's Office:

This form is to be used when data controllers wish to report a breach of the Data Protection Act to the (DPA).

If you are unsure whether it is appropriate to report an incident, you should read the following guidance before completing the form: Notification of Data Security Breaches to the Information Commissioner's Office.

Please provide as much information as possible and ensure that all mandatory (*) fields are completed. If you don't know the answer, or you are waiting on completion of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant supporting information, eg incident reports.

In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

- **Organisation details**
- *What is the name of your organisation – is it the data controller in respect of this breach?*
- *Please provide the data controller's registration number.*
- *Who should we contact if we require further details concerning the incident? (Name and job title, email address, contact telephone number and postal address).*

- **Details of the data protection breach**
- *Please describe the incident in as much detail as possible.*
- *When did the incident happen?*
- *How did the incident happen?*
- *If there has been a delay in reporting the incident to the ICO please explain your reasons for this.*
- *What measures did the organisation have in place to prevent an incident of this nature occurring?*
- *Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.*

- **Personal data placed at risk**
- *What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.*
- *How many individuals have been affected?*
- *Are the affected individuals aware that the incident has occurred?*
- *What are the potential consequences and adverse effects on those individuals?*
- *Have any affected individuals complained to the organisation about the incident?*

- **Containment and recovery**
- *Has the organisation taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.*
- *Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.*
- *What steps has your organisation taken to prevent a recurrence of this incident?*

- **Training and guidance**
- *As the data controller, does the organisation provide its staff with training on the requirements of the (Data Protection framewok)? If so, please provide any extracts relevant to this incident here.*
- *Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?*
- *As the data controller, does the organisation provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.*

- **Previous contact with the (DPA)**
- *Have you reported any previous incidents to the (DPA) in the last two years?*
- *If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the (DPA) reference number.*

- **Miscellaneous**
- *Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.*
- *Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.*
- *Have you informed any other regulatory bodies about this incident? If so, please provide details.*
- *Has there been any media coverage of the incident? If so, please provide details of this.*

Sending this form:

Send your completed form to (email of the data protection authority).

PROPOSITION FOR A TEMPLATE: REGISTER OF DATA BREACHES

1	Date of breach	
	Date when breach was actually discovered	
	Name of reporting person/contact details	
	Summary of the event and circumstances	
2	What does the Data breach consist in?	*(Confidentiality/Availability/Integrity)*
3	Type and amount of personal data affected	
4	Procedures/instructions in place to minimise risks to security of data/CURRENT ACTIONS TAKEN TO ENCOUNTER DATA BREACH	
5	Does the incident need to be reported to the CNPD? When was it reported?	
6	Does the incident need to be communicated to data subjects Ref. of communication made/Date of release of communication	
7	Foreseen procedure changes to reduce risks of future data loss	
8	Others	
9	CONCLUSION	

APPENDIX III
ACTION PLAN – IN BRIEF

By now, financial stakeholders are already implementing their **Plan of action** to abide to the aforementioned rules and guidance to comply with the Regulation. Such plan of action was most certainly encompassing the following key criteria; as the case may be, one may always refer to the actions pinpointed below.

▶ IDENTIFY

Members shall first identify their processing by defining who is actually involved in the processing, establish a list of their processing together with their defined purposes and correlated lawfulness criterion/criteria. The controller may use more than one criterion to make sure that its processing will not be challenged by the data subject. It shall then be determined if a transfer of data will be operated, within the EEA or elsewhere and how long the data will be kept for.

▶ ASSESS

The controller will evaluate where it stands compared to the new Regulation's requirements pinpointed supra. One may for example appoint/require a Data Protection Officer to implement the necessary procedures and advise the management board, carry on data protection impact assessments as the case may be, evaluate its binding corporate rules to see if fit with the Regulation's demands. A Risk analysis shall in addition be carried on.

▶ ADAPT

Members shall thereafter proceed to the update of their contractual clauses, general conditions (data subjects/third parties/contractors), always bearing in mind the new rights conferred upon the data subjects by the Regulation, mostly with a view to increase information provided to the latter, enabling them to effectively exert their rights and managing the clients' consent for processing.

Procedures/processes/IT systems and security shall be updated and/or reorganised **to make sure that the accountability principle** is duly applied by the controller.

▶ DEMONSTRATE AND PLAY BY THE RULES

Make sure that you are able show your abidance to the core principles of the Regulation, especially to the data protection authorities. To this end, set up notably records of processing activities, proceed to the training of your staff etc…

The few concrete suggestions emphasised below may be useful in stepping further into the Regulation:

- **Carry out internal audits** to identify the processing of personal data, the work streams and the stakeholders.
- **Carry out gap analysis** of the identified processes for handling new and current data protection obligations.

- **Review existing information notices** to safeguard the accurateness, comprehensiveness, and up to date criteria. Evaluate whether or not **any additional information will be required** under the Regulation.
- Ensure that all the relevant staff receives **training** on data protection. The records to prove the training shall be kept properly to be prepared in the case of claims of negligence or malicious actions.
- **Updating customers regularly on data processing methods is crucial**. Additionally in the event of a change in such methods, informing customers, if not done so yet, in writing will be essential.
- Be able to **collaborate on the data collection, storage and erasure with the relevant departments/units of the controllers**.
- Assessment and **minimisation of risks** should also be part of the adaption process. The controllers can carry out such risk assessment and minimisation by conducting privacy impact assessments (including the whole life cycle of data) on data processing and the supporting IT systems.
- **Update the relevant contracts** by taking into account the new data protection requirements will also be necessary for adaption. The internal registers that have the data related to the employees have to be reviewed and updated. Additionally, the data protection policies for the employees of the controllers will also have to be updated accordingly.
- As mentioned above, **be prepared for the events in case of a data breach** is crucial. The preparation of a crisis management plan that sets out the rules of data breach notification will be useful for the controllers when they face a data breach.
- **Make sure that your systems fulfil the «right to be forgotten», «right to erasure» and the «right to data portability»** of your data subject in accordance with the Regulation. Therefore, a **tailor-made strategy** that covers data classification, retention, collection, destruction, storage and search will be required for each controller. Such strategy that is included in internal procedures will have to cover all channels by which data is collected, including the internet, call centres and paper.
- **Align the HR and data protection rules** in order to provide compliance with the new requirements. Kindly refer to the separate Guideline of the ABBL devoted to this specific topic.
- **Develop guidelines for information requests and inspections** by a DPA and preparation of the staff for potential inspections.
- **Follow up actions and announcements** of the relevant competent DPA.
- Appoint a **DPO** in cases that are deemed as necessary.
- Elaborate a DP Governance tool together with appropriate relevant controls.

Office address:

ABBL a.s.b.l.
12, rue Erasme
L-1468 Luxembourg

Postal address:
P.O. Box 13, L-2010 Luxembourg

Tel.: (+352) 46 36 60-1
Fax: (+352) 46 09 21

mail@abbl.lu
www.abbl.lu