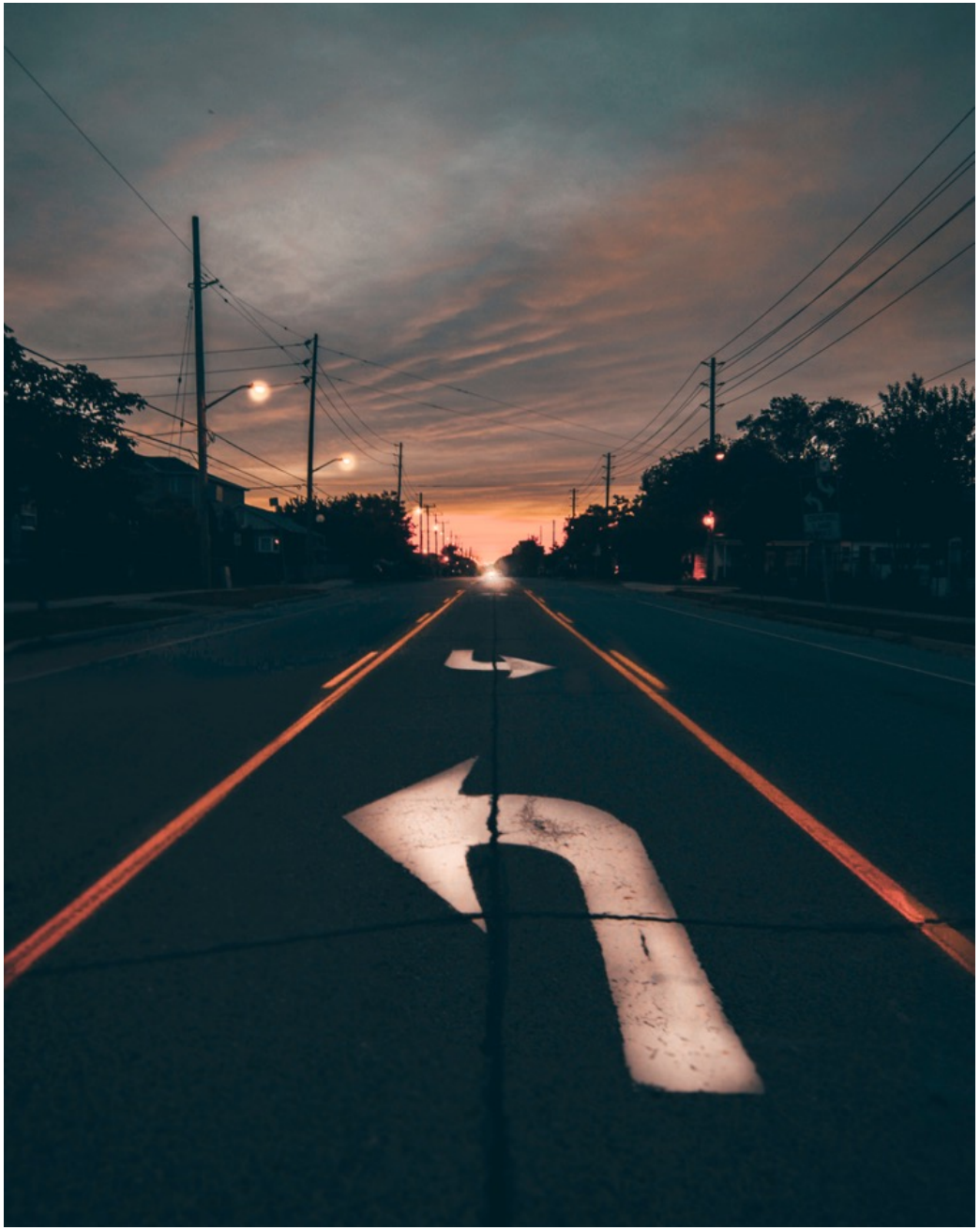
GDPR

General Data Protection Regulation

COMING INTO FORCE the
24th of MAY 2016

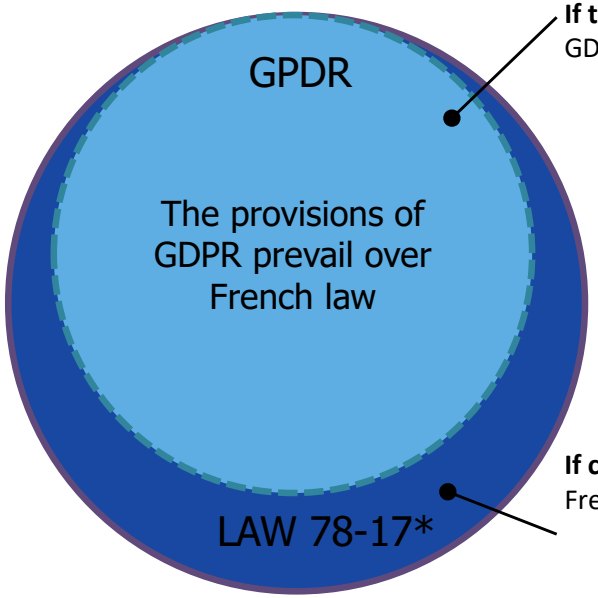
APPLICABLE
FROM the
25th of MAY 2018

SUMMARY



1. Applicable set of rules

GOALS
Harmonizing & enhancing the protection of personal data
Establish a single legal framework for the EU



If there is an incompatibility:
GDPR will prevail over French law

If compatible:
French law will also by applied

Draft law 490: keep an eye on it : It can be more restrective

Application of GDPR and national law

Competent authority in France: Commission Nationale de l'Informatique et Liberté (CNIL)

- Administrative Authority
- Mission: Information, control and advice

GDPR renders national laws and regulations incompatible with its inapplicable provisions.

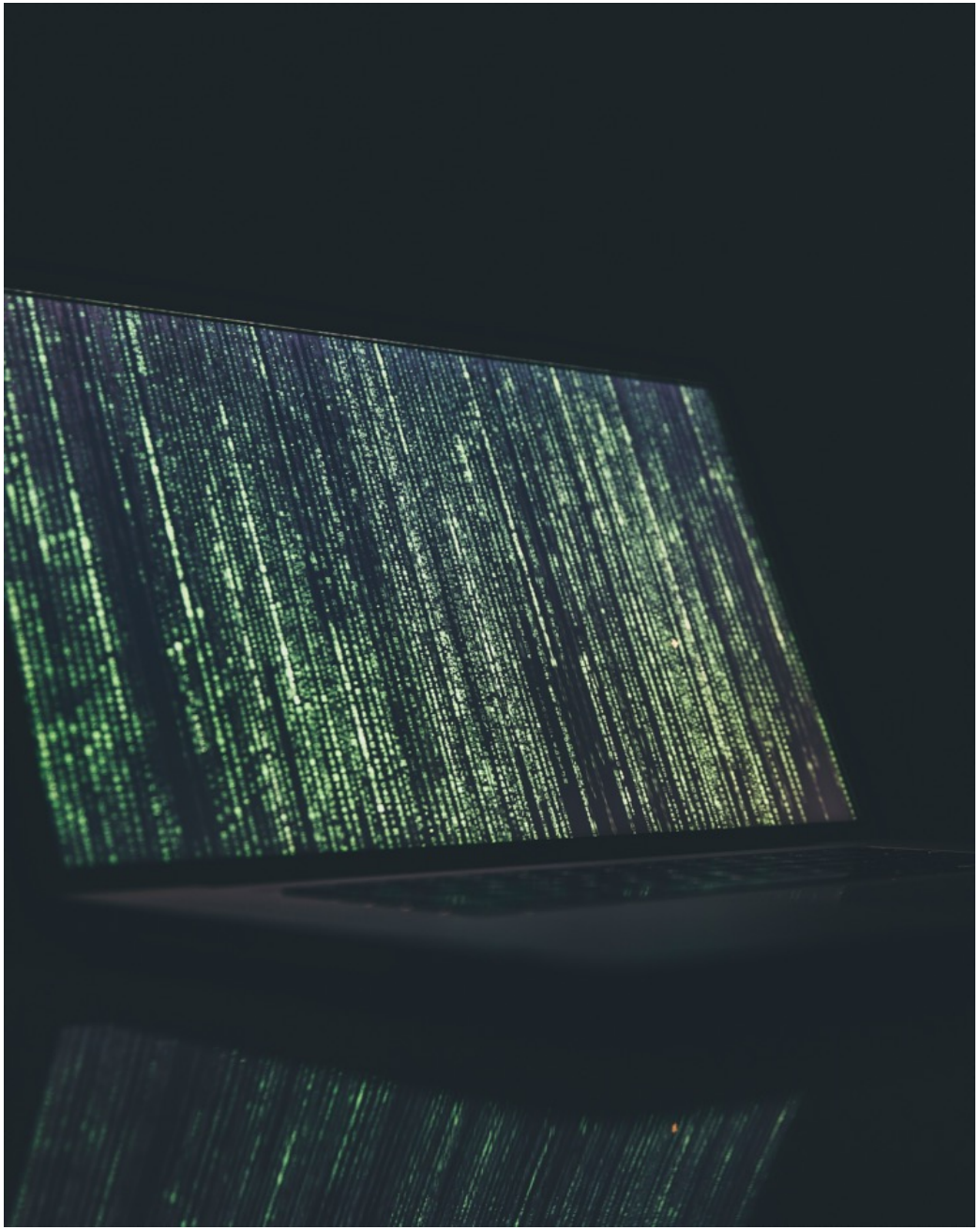
It has a superior position in the hierarchy of norms, but does not have the ability to repeal French laws.

The regulation is directly applicable in each Member State (art. 94). It contains numerous references to the national law of the Member States, which will be intended to supplement the normative framework of GDPR.

GDPR repeals Directive 1995/46/EC for the protection of data with regard to personal processing and on the free movement of such data.

To avoid discussions on the notion of incompatibility: a reform of the French Data Protection Act is necessary in order to not render a certain number of provisions of GDPR inapplicable.


ARE YOU AFFECTED BY
GDPR ?



STEP N°1:
Determine the type of data

GDPR extends and clarifies the territorial scope of EU data protection legislation

Is there any **processing** of **personal data** ?

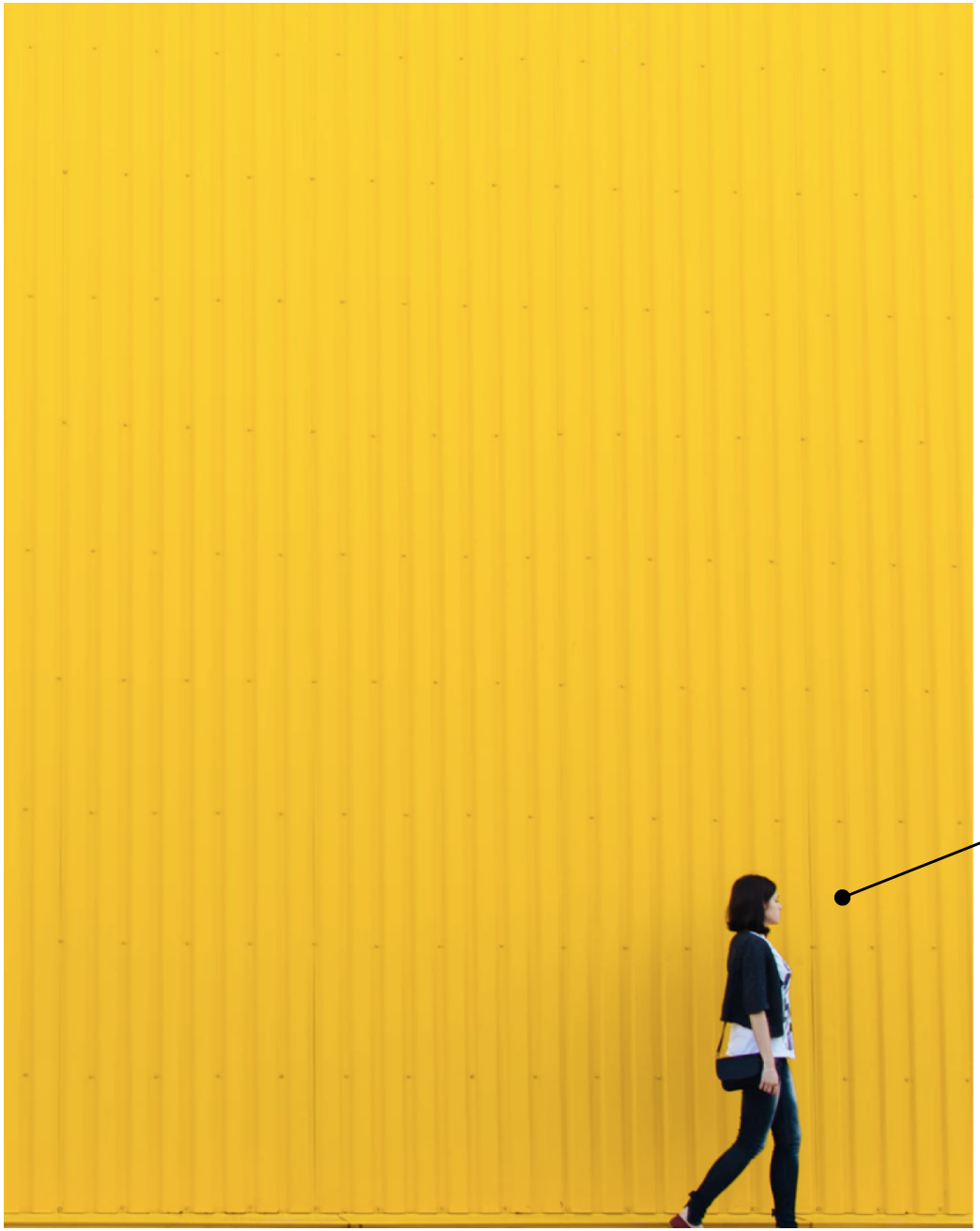
- Processing "any operation or set **of operations, whether or not carried out using automated processes** and applied to personal data or data sets".

- Personal data "means any information relating to a **natural person**, whether identified or **simply identifiable** (even indirectly, for example, by an identifying number or a cross-check of information) ".

NB: Will apply to the processing of personal data, whether automated (even partially) or not (provided that the data processed is contained in or will be included in a file).

Not concerned:

- Treatments for private use only;
- Certain processing operations carried out by Member States and/or competent authorities for the purpose of prevention;
- Execution of criminal sanctions.



DEFINITIONS

What is personal data (art 4)?

- Identity
- Contact details
- Identification number – Badge
- Localization data
- IP Address
- Consumption habits
- Information about professional life
- Email address

Art. 2-1) 4-2)

DEFINITIONS

What is automated and non-automated processing of personal data?

Collection	Recording	Organization	Structuring (see Big Data)
Conservation	Adaptation	Modification	Extraction
Consultation	Use	Communication	Broadcasting
Availability	Reconciliation	Interconnection	Limitation
Erasing	Destruction	Seizure	Use for a test

STEP N°2:

Identify who must comply with the regulations

Data subject

- GDPR imposes obligations on the parties responsible for processing and also on entities processing data on behalf of a third party **(regardless of the nationality of the data subject)**

Controller

- The natural or legal person, public authority, department or other party which, alone or jointly with others, determines the purposes and means of the processing; where the purposes and means of such processing are determined by Union law or the law of a Member State, the controller may be designated or the specific criteria applicable to its designation may be provided for by Union law or by the law of a Member State.

Processor

- The natural or legal person, public authority, department or other party processing personal data on behalf of the controller (including free of charge)

STEP N°3:
Geographic

Processing of data by a controller or processor on EU territory

Processing of data belonging to data subjects residing in the EU by a controller or processor who is not established in the EU, where the processing activities are linked

- To supply goods or services to these persons concerned within the EU
- Or to monitor the behavior of these people

Processing of data by a controller who is not established in the EU, but in a place where the national legislation of a Member State applies under public international law

KEY PRINCIPLES
IN PERSONAL DATA MATTERS (I)

PRINCIPLES ON DATA	DEFINITIONS	IN PRACTICE	EXAMPLES
Transparency	Data processing: Faithful, lawful and transparent	The rights of the data subjects must be respected, which means that there must be no collection, use, consultation, or processing of data without full disclosure of the processing to the data subjects.	Collection form in clear terms: the content of the information to be provided is specified in the GDPR
Limitation of Purposes	Collection for specific, explicit and legitimate purposes	Collection for a specific purpose and must not be reused at a later date for another purpose other than that originally intended	Data collected by a health care institution to monitor the condition of patients may not be used for canvassing operations without prior precautions: risk of misuse of purpose(s).
Security and Confidentiality	Data processing to ensure appropriate security	Guarantee security by means of appropriate organizational and technical measures, to prevent data from being distorted, damaged, or accessed by unauthorized third parties.	Organization: formalizing a data security policy, raising staff awareness, ... Techniques: HTTPS protocol For CC numbers: store in hashed form with secret key use

KEY PRINCIPLES
IN PERSONAL DATA MATTERS (II)

PRINCIPLES ON DATA	DEFINITIONS	IN PRACTICE	EXAMPLES
Minimization	Data relevant, adequate, and limited to what is necessary for the purposes for which it is processed	Personal data must only be processed if the purpose of the processing cannot be achieved by other means.	Advertising on a website to allow internet users to receive free quotes / documentation, can collect the identity and contact information of the applicant to answer the request but not banking data, even if it is to anticipate a future relationship.
Exactitude	Accurate and regularly updated data (correction, see deletion)	Reasonable steps must be taken to ensure that inaccurate data is rectified or erased.	Establish a process for regular review of data to determine whether it is still relevant or obsolete.
Storage limitation	Storage for a period not exceeding that which is necessary in view of the purposes for processing it	Limitation to the strict minimum (identification elements of employees must not be kept more than 5 years after the employee's departure, elements relating to the movement of people must not be kept more than 3 months, ...)	A true data retention, archiving, and purging policy must be formalized.

KEY PRINCIPLES
IN PROCESSING MATTERS (I)

ALTERNATIVE CONDITIONS	DEFINITIONS	IN PRACTICE	EXAMPLES
Consent of the data subject	- Positive and unambiguous act (should not give way to uncertainty) - Free: freedom of choice: - Specific: for precise purpose - Informed: after receiving information in order to make an informed decision	- Consent to process data for the purpose of sending newsletters by email; - Employee consent to use their photograph as part of an internal social network.	***Valid consent:*** - Checkbox / special technical parameter setting - In all cases: Consent must be obtained separately from other agreements or other information ***Invalid consent:*** - Cases of silence - Default pre-checked boxes - Implicit or purely passive agreement
Execution of a contract	Necessary in connection with a contract or the intent to enter into the contract	Beware of restrictive interpretation: covered by a contract does not automatically mean necessary for its execution.	- Processing employee data so that the employer can pay them - Postal address processing of a customer so that products purchased online can be delivered.
Legal obligation **Execution of a public interest or public authority mission**	In accordance with a legal obligation to which the controller is subject or necessary for the performance of a public interest task	The obligation must come from European legislation or that of a Member State on which the controller depends. If imposed by a third country: does not fall under this provision	Processing of data relating to their employees' remuneration by employers so that they can communicate them to the social security or tax authorities.

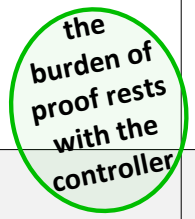
KEY PRINCIPLES
IN PROCESSING MATTERS (I)

ALTERNATIVE CONDITIONS	DEFINITIONS	IN PRACTICE	EXAMPLES
Vital interest	Vital interest of the data subject or other natural person is at stake	This notion appears to be limited to life or death issues or threats that involve a risk of injury or harm to health.	Data treatment in the framework of humanitarian work
Legitimate interest	Processing is necessary for the legitimate interests of the controller or a third party, unless the interests or freedoms of the data subject prevail.	Balance between the controller's interest (economic interest, security, fraud prevention, etc.) and those of the data subject or third parties (life, privacy, damage to his or her reputation, etc.) – Proof must be provided by controller, who must inform the person of the legitimate reasons for processing when on this basis. – The person may object to it at any time	Data processing for fraud prevention purposes

RIGHTS OF THE DATA SUBJECT


Deploy the necessary measures for compliance

MEASURES TO BE IMPLEMENTED

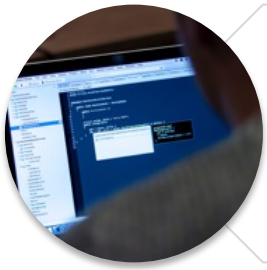
PRINCIPLES O PROCESSING	DEFINITION	IN PRACTICE	EXAMPLE
Accountability 	Obligation to implement internal mechanisms and procedures to demonstrate compliance with the rules on the protection of personal data in accordance with the regulation, and to be able to demonstrate this.	Organization within the company by means of concrete measures: adapted documentation, written and binding data processing policy, verification procedures to ensure the effectiveness of the implemented measures.	Charter for the use of personal data + booklet+ guide, drafting code of conduct, appointing a DPO
Privacy by design **(a new concept that contributes to Accountability)**	The need to take appropriate measures to take concrete account of data protection in projects from the outset and to ensure that the products and services offered comply with data protection and freedom provisions throughout their lifecycle.	Obligation to implement internal mechanisms and procedures to take data protection into account from the design stage - from the start of the project	1. Development of a methodology/procedure integrated in the organizational processes 2. Specifications reflecting the legal constraints to be respected in all new projects (see table on principles) 3. Validation mechanism to ensure data protection compliance 4. Implementation of appropriate tools 5. Setting up an adapted organization
Privacy by default **(a new concept that contributes to Accountability)**	Consists of taking appropriate technical and organizational measures to ensure that, by default, only the data necessary for the specific purpose of the processing operation is collected and used.	Default settings must ensure that the highest possible data protection is guaranteed.	ex: application requiring geolocation - The user will be able to modify the parameters (location) at will, even if notified of the dangers of these changes.

Data Protection Officer (DPO)

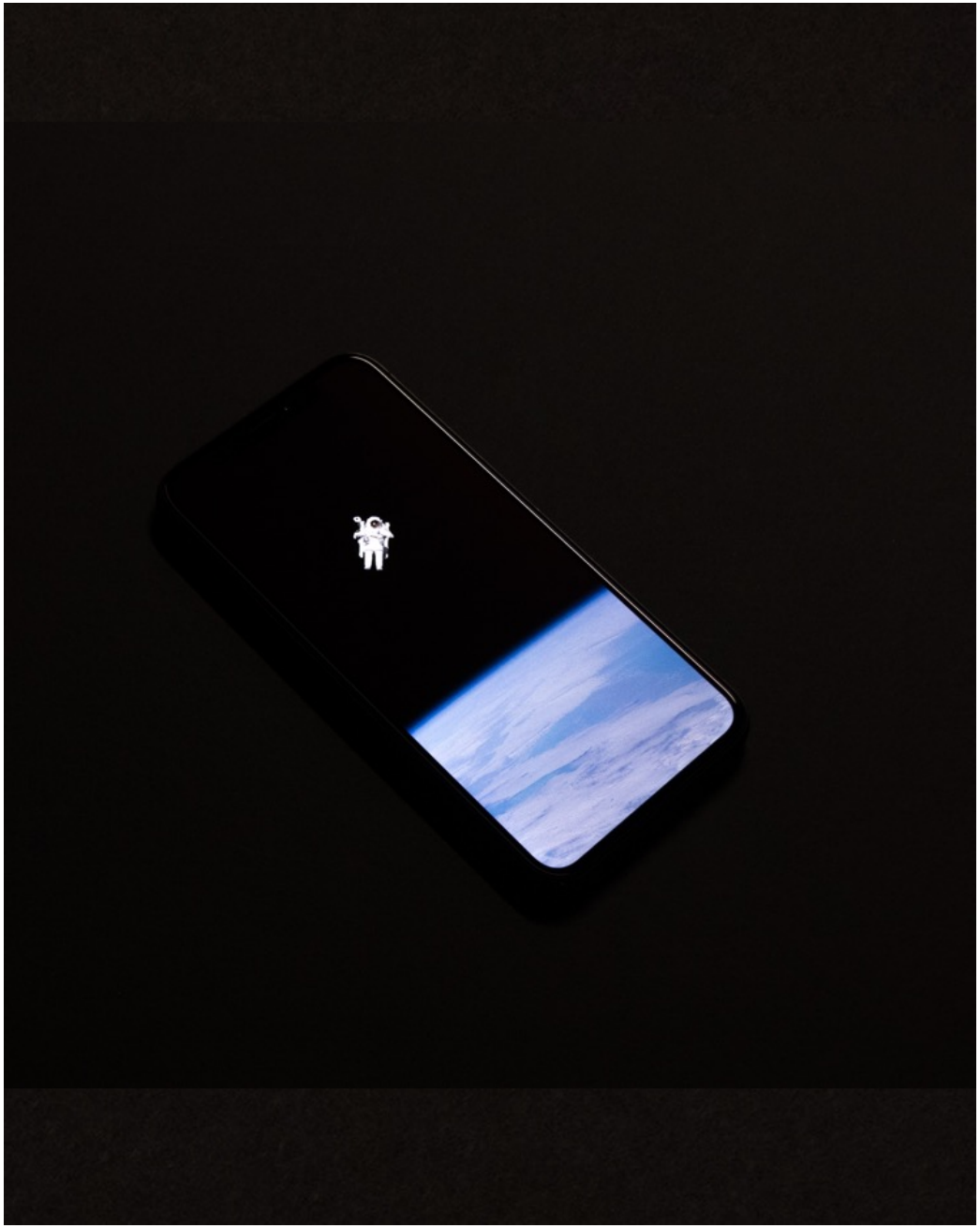
THE CASE OF A MANDATORY DESIGNATION

The basic activities of the controller or processor shall consist of processing operations which, by their nature, scope and/or purpose, require regular and systematic large-scale monitoring of data subjects.

Public body or authority, except courts acting in the exercise of their judicial function

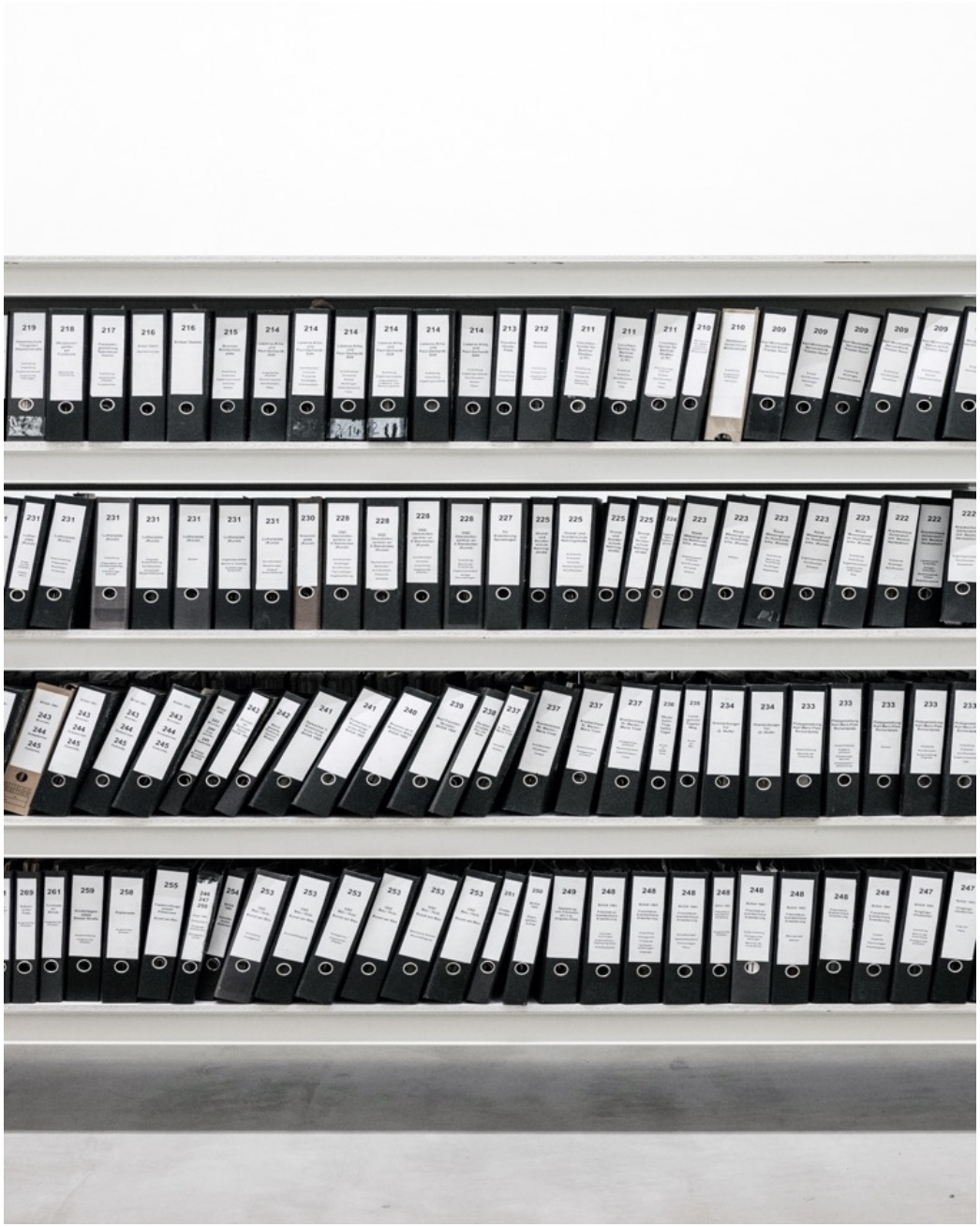


The basic activities of the controller or processor consist of large-scale processing of sensitive and personal data relating to criminal convictions and offenses.



TASKS OF THE DPO

Inform and advise	•on the obligations of the controller, processor or employees processing personal data deriving from the regulation and the provisions of the Union or the Member State concerned
Control	•compliance with the regulation and other Union or Member
State provisions	•compliance with internal data protection rules
Consultant	•for carrying out impact assessments
Cooperate	•with the supervisory authority
Practice	•the function of contact point for the supervisory authority



WHY KEEP RECORDS?

- To meet the accountability constraint, processing must be recorded in a processing activity log.
- Updated regularly as new treatments or modifications to existing treatments are implemented.
- Must be made available to the supervisory authority upon request

TRAPS TO AVOID !

- Regulation: record keeping is not mandatory for entities with fewer than 250 employees
- Temptation for small and medium-sized enterprises to stick to this exception in order to escape this obligation
- Beware of exceptions: there must be a register (regardless of the number of employees) if the processing operation is likely to pose a risk to the rights and freedoms of data subjects, if it concerns so-called "special" data or data relating to criminal offenses or convictions or if it is not occasional.
- Any processing carried out which has a certain durability must be included in a register of processing activities, whether the entity has more or less than 250 employees.

THE INFORMATION IN THE RECORD

CONTROLER	PROCESSOR
Identity and contact details of the controller, their representative, and the data protection officer	Identity and contact details of the processor, their representative, each controller and their representative(s), and the Data Protection Officer
Processing purposes	Processing categories
Categories of data subjects	x
Categories of processed data	x
Categories of data recipients	x
Existence of data transfers outside of the EU and reference to the safeguards associated	
General description of the technical et organizational safety measures put in place	
Data retention duration	

Records for Controller

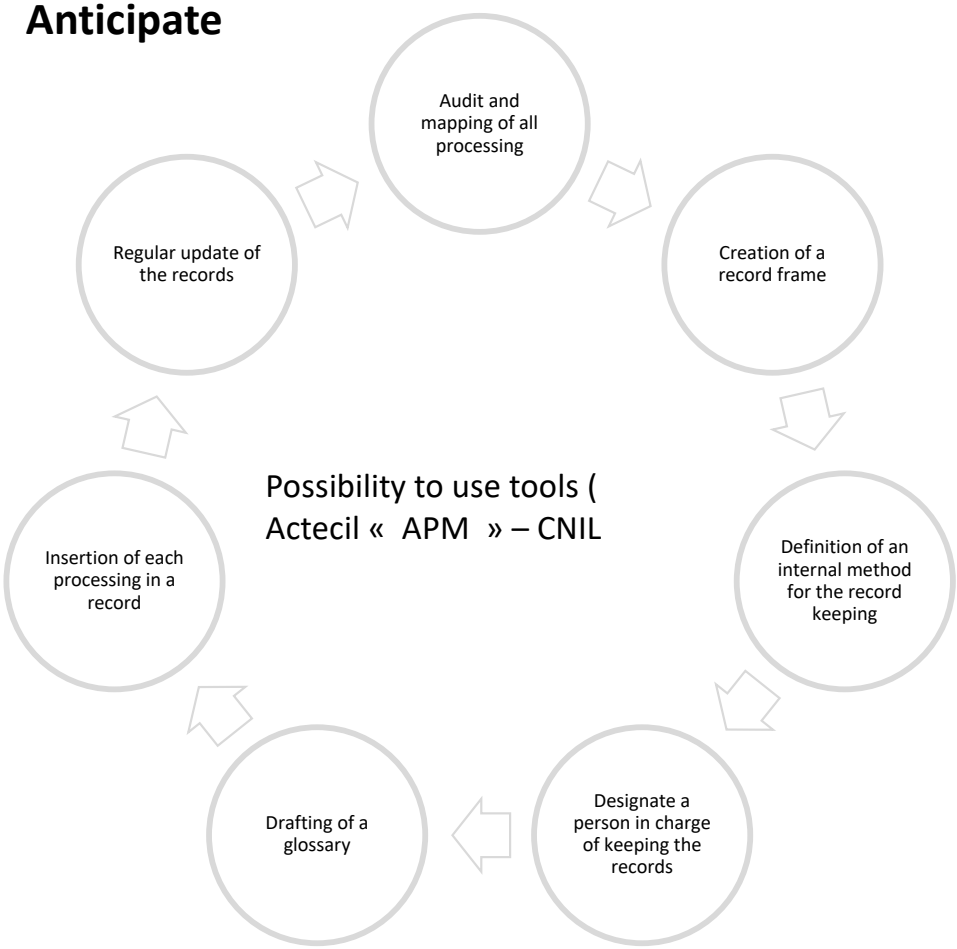
Processing n°1	**Indicate the name of the treatment or the internal reference**
Creation date : **Date of update**	Indicate the actual date of implementation. In the case where prior formalities with the CNIL have been necessary, indicate the date of the receipt. Indicate the date of update when there is a substantial change in the initial treatment.
Main purposes of the processing	Indicate here the main objectives pursued by the data processing operations
Detail of the purposes of the Processing **Sub-purposes**	Detail the essential components of the general purpose and sub-purpose. *For example, it is a software : indicate its functionalities*
Actors **Controller** **Data Protection Officer** **EU representative** **Joint responsible person(s)**	Indicate the actors involved in the processing operation and their contact details. *For example: name, address, PC, city, country, phone, e-mail address, etc.*
Function of the person or department with whom the right of access is exercised	Who is responsible for the access to the right of access in the service? Any person has the right to request the communication of data concerning him or her, who is in charge of this type of request?
Security measures	Indicate the technical and organizational security measures implemented to minimize the risks of unauthorized access to data and the impact on the privacy of data subjects. *For example: management of authorizations, authentication, logging, encryption, IT charter, etc.*
Categories of persons concerned by the processing operations	Who owns the processed data, who has communicated them? *For example: customers, employees, candidates, users*
Categories of processed data	<u>Data Categories</u> - Civil status, identity, identification data, images.... - Personal life (life habits, family situation, etc.) - Economic and financial information (income, financial situation, tax status, etc.) - Login data (IP address, logs, etc.) <u>Duration of the storage</u> Specify, for each category of data, how long you keep them.

Records for Processor

Processing n°1	**Indicate the name of the treatment or the internal reference**	
Creation date : **Date of update :**	Indicate the actual date of implementation of the processing operation on behalf of the controller. Indicate the date of update when there is a substantial change in the initial treatment.	
Categories of processing operations carried out on behalf of the controller	Indicate here the categories of processing operations carried out on behalf of each controller.	
Détail des finalités du Traitement, **Sous-finalités,** **Fonctionnalités**	Detail the essential components of the general purpose and sub-purpose. *For example, if it is a software, indicate its functionalities.*	
Actors **Subcontractor** **Controller on whose behalf the processing is carried out** **Data Protection Officer** **EU representative**	Indicate the actors involved in the processing operation and their contact details. *For example: name, address, PC, city, country, phone, e-mail address, etc.*	
General description of security measures	Indicate the technical and organizational security measures implemented to minimize the risks of unauthorized access to data and the impact on the privacy of data subjects. *For example: management of authorizations, authentication, logging, encryption, IT charter, etc.*	
Transfers outside of the EU	<u>Country of destination</u> Identify data transfers outside the European Union.	<u>Type of guarantees</u> *For example: standard contractual clauses, adequate level, BCR, etc.*

HOW TO ORGANIZE YOUR RECORDS

Anticipate

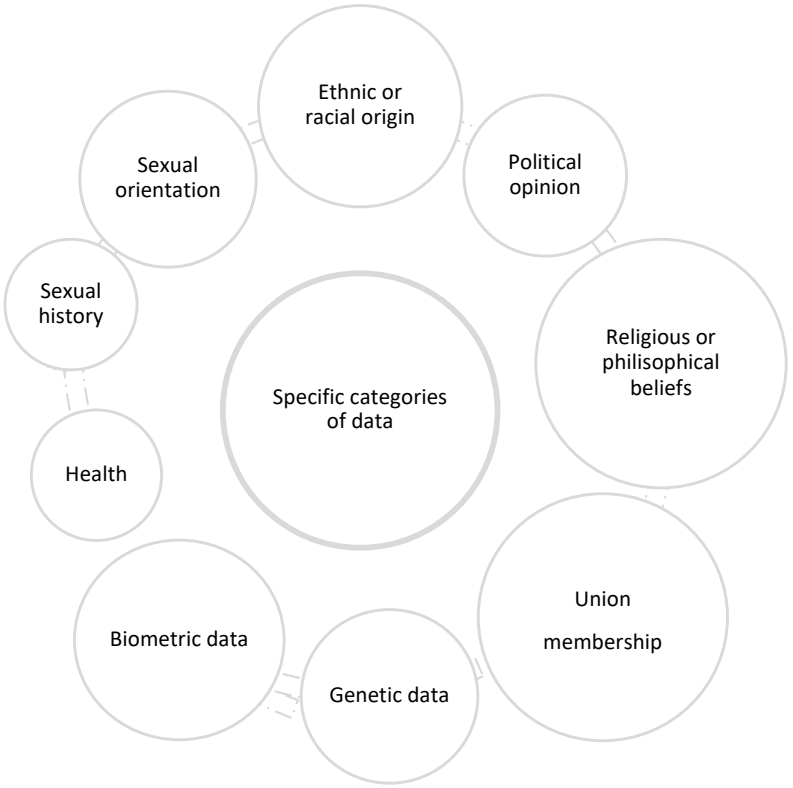



Is the treatment likely to create a high risk for the data subject?

SPECIFIC CATEGORIES OF DATA

The novelties of the GDPR

Due to the quality of the data, and in particular when dealing with specific categories of data, special obligations may be imposed, such as an impact assessment or the opinion of the CNIL.



WHEN SHOULD YOU DO AN IMPACT ASSESSMENT?

	Treatments concerned	
Treatments presenting particular risks by virtue of their nature, scope, or purpose	Treatments presenting particular risks: - large scale systematic monitoring of an area accessible to the public, - large-scale processing of sensitive information, - assessment of personal aspects based on automatic processing and allowing decisions to be made about a person...	Treatments considered by the supervisory authority as being likely to present specific risks to the rights and freedoms of data subjects (public list)

Example of risky processing : video protection

ANALYSIS IN PRATICE

General description of the envisioned processing and purposes

Assessment of the necessity and proportionality of processing operations

PLUS

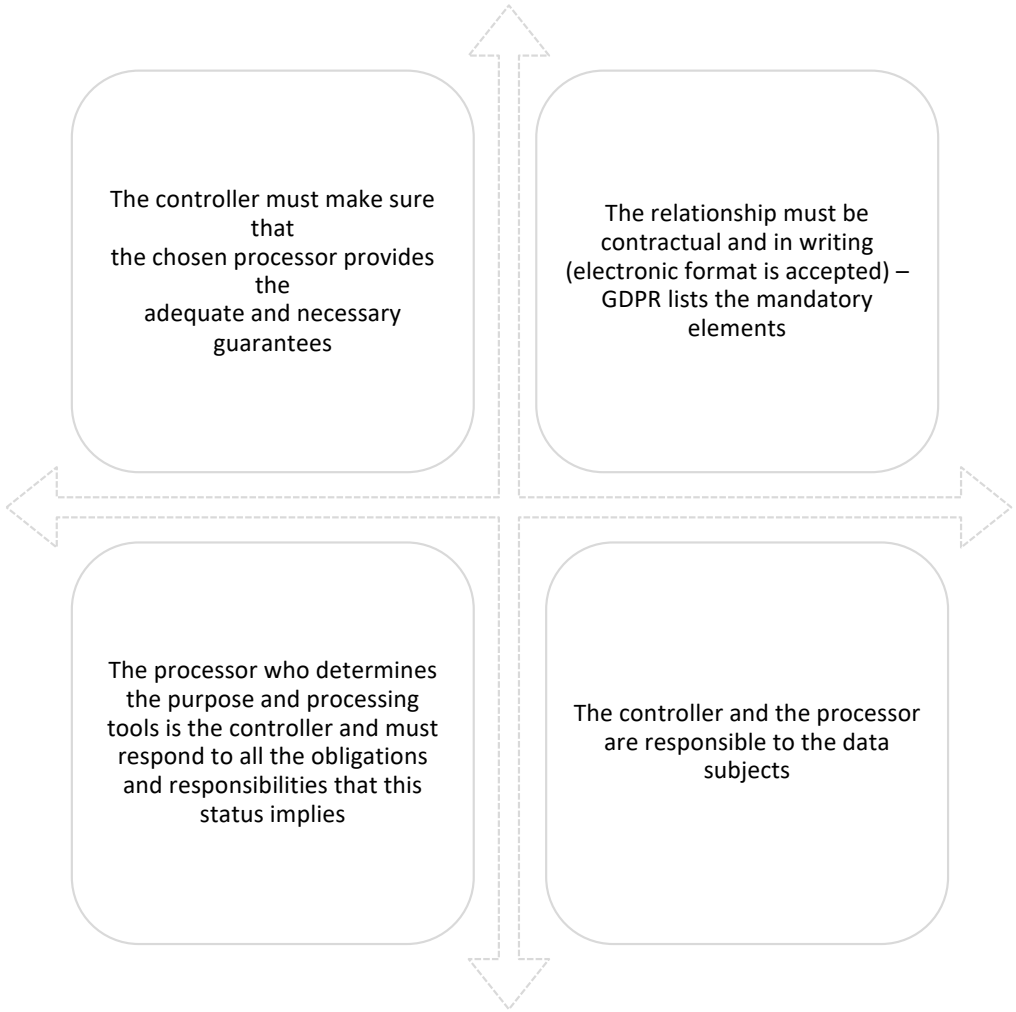
Prior consultation with the data protection authority if the result of the analysis indicates that the processing presents a high risk.

Risk assessment of data subjects' rights and freedoms

Envisioned measures to face the risks


HOW TO ORGANIZE THE RELATIONS
BETWEEN
THE PROCESSING PARTIES

REBALANCING THE RELATIONSHIPS



WARNING

The processor shall immediately inform the controller if, in his or her opinion, an instruction constitutes a breach of the GDPR or other provisions of EU law on data protection.

Verify the legality of the instructions received

The processor is only responsible if

or

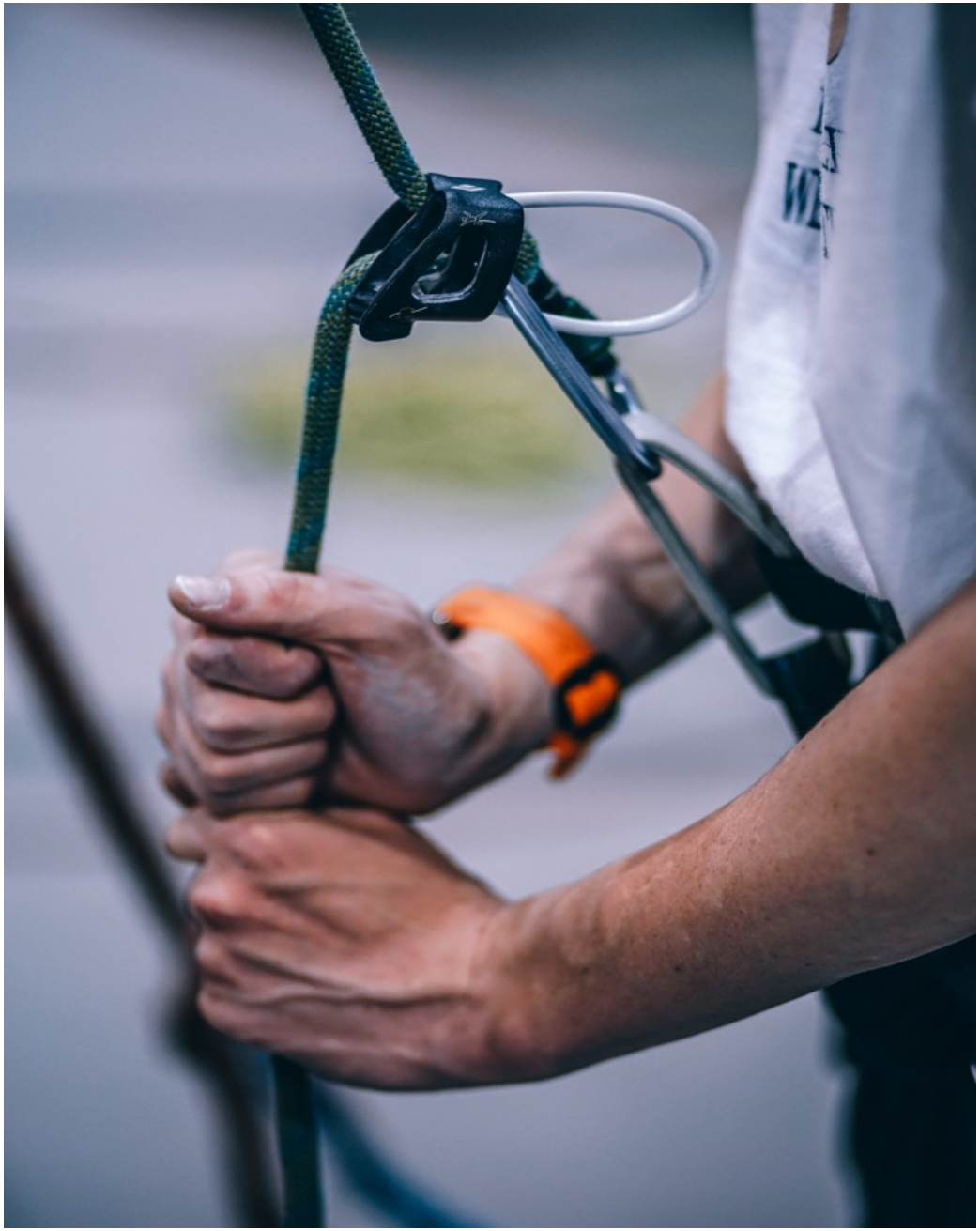
or

He did not respect the obligations set out in the GDPR

He acted outside the lawful instructions of the controller

He has acted contrary to The controller's instructions

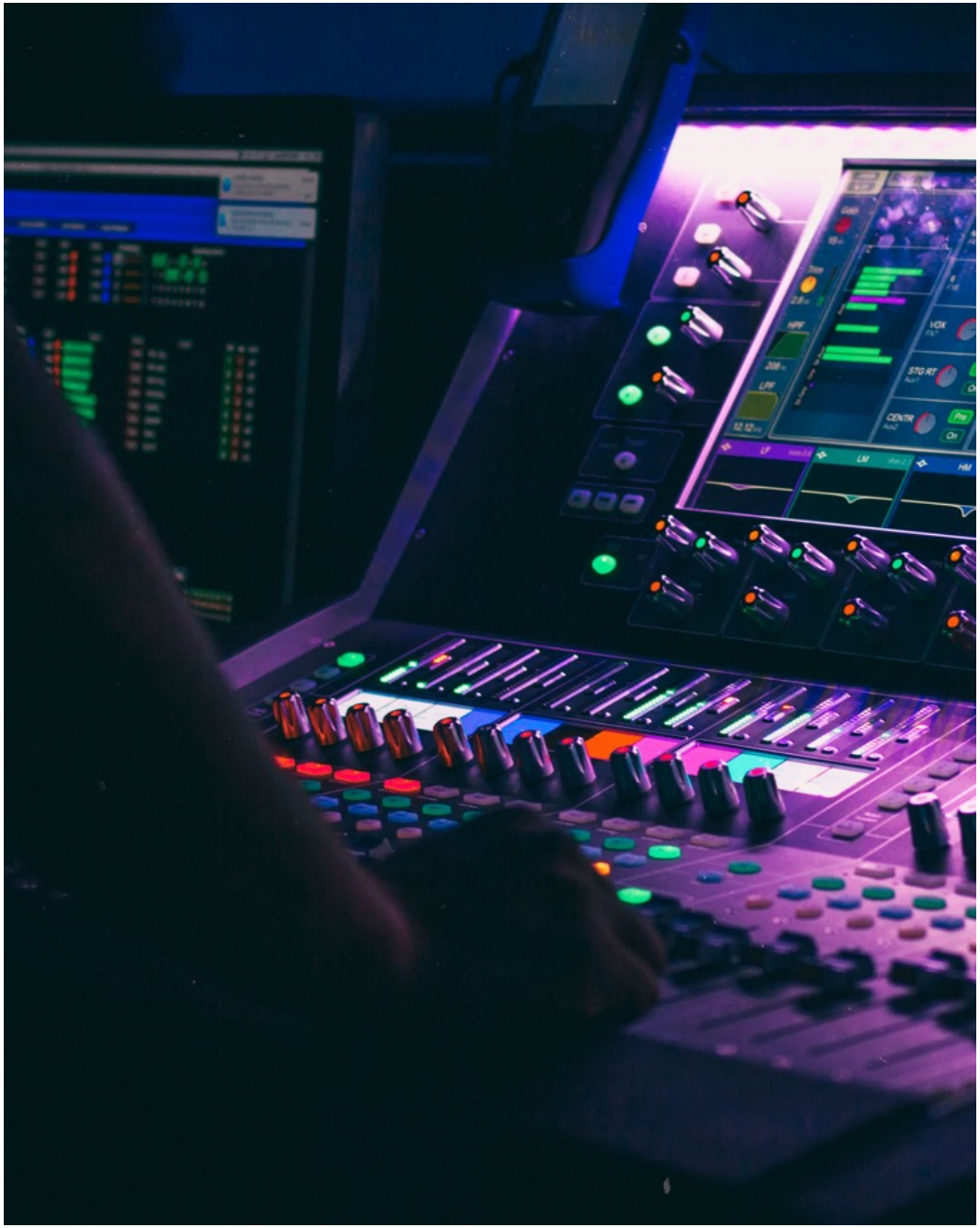

The security obligation



DEPLOYING APPROPRIATE SECURITY AND CONFIDENTIALITY MEASURES

- Security policy (art.32)

Duties of the controller and processor



PRACTICALLY

Formalize a security breach management procedure describing the main steps: identification and correction of a breach, filing of a complaint, insurance claim, ...

Drafting model templates: notification to the supervisory authority, communication to the data subject

Develop a documented record of security vulnerabilities with constructive feedback

MANAGEMENT OF SECURITY VULNERABILITY REGARDING DATA

Duty N° 1

Duty of the controller

Unless the violation is not likely to create a risk to the rights and freedoms of data subjects

- Within 72 hours to the public authority
- Directly to the data subjects

Duty N° 2

Duty of processor

The processor notifies the controller of any breach of personal data

- Within the best delay possible after learning about it

MANAGE THE TRANSFER OF DATA OUTSIDE THE EU

Principle: Transfers of personal data outside of the European Union territory are prohibited unless the destination country or recipient provides an adequate level of protection.

It should be noted that this ban on transfers does not apply to Iceland, Liechtenstein and Norway, since these countries have transposed the provisions of Directive 95/46/EC into their national legislation (these countries and the 27 Member States of the European Union constitute the European Economic Area).

This ban does not apply to transfers to countries recognized by the European Commission as "adequate".

To date, this has been the case in: Andorra, Argentina, Canada, the Faroe Islands, the Isle of Man, Guernsey, Jersey, Israel, Uruguay and Switzerland.

MANAGE THE TRANSFER OF DATA OUTSIDE THE EU

For transfers out of these countries, several tools have been developed to enable players to provide a sufficient level of protection: binding corporate rules (or BCR), standard contractual causes, and adherence to the principles of "Privacy Shield".

The law also provides for exceptions allowing data to be transferred to third countries without a sufficient level of protection.

All of these mechanisms are presented in the CNIL guide in order to answer questions from the public about the transfer of personal data outside the European Union.

MANAGE THE TRANSFER OF DATA OUTSIDE THE EU

Map that allows you to visualize the different levels of data protection in countries around the world

https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

SANCTIONS

- Lack of data protection from the design stage and data protection by default
- Absence of an established representative in the European Union
- No record of processing activities
- Lack of cooperation with the supervisory authority
- Failure to notify the supervisory authority or data subject of a data breach
- Lack of impact assessment

€10,000,000
or
2 % annual global turnover

- Non-compliance with the basic principles of a processing operation (legitimacy, fairness, adequacy, and relevance of data, consent, sensitive data, etc.)
- Failure to respect the rights of individuals
- Non-compliance with the rules on transfers of personal data

€20,000,000
or
4 % of annual global turnover

ELEMENTS TAKEN INTO ACCOUNT

- Nature, seriousness and duration of the violation
- Category of personal data concerned
- How the supervisory authority became aware of the violation
- Number of people concerned and level of damages suffered
- Degree of cooperation with the supervisory authority
- Measures already ordered against the controller or processor
- Deliberately or negligently committed violation
- Previously commited violations
- Application of codes of conduct or certification mechanisms
- Measures taken to soften the damages suffered
- Level of responsibility given the technical and organizational measures implemented
- Other aggravating or mitigating circumstances

➢ Advice : start your compliance and keep in mind that you have to demonstrate your good faith by all means

GDPR

Focus on the hosting of data

BeSafe
Save & Safe

Hosting and GDPR

What are the services involved ?

The main providers of hosting services

- Collaborative messaging (MS Office 365, Echange)
- Document sharing (Dropbox, Wetransfer)
- Hosting of private servers (virtual machines)
- Hosting of applications (SaaS)
- External backup (BaaS)
- Websites (E-commerce, social networks, etc.)

In its current version, GDPR
does not provide a clear answer

Nevertheless, in line with GDPR, a new regulation concerning e-commerce will appear:

The E-Privacy

E-Privacy

What will change for website operators

- Requirement to document compliance with GDPR
- More complex agreements and authorizations
- Privacy by Design and Privacy by Default Principles
- Extension of rights to information and dereferencing (deletion of data)
- The right to transferability of data
- Much more extensive information requirements (ex: the data protection declaration of a website)

Today	Tomorrow
The user must accept cookies to have access to the website	If the user refuses the cookies, the content of the website must appear nonetheless

➢ E-Commerce is the first step of regulation, so you have to take the lead

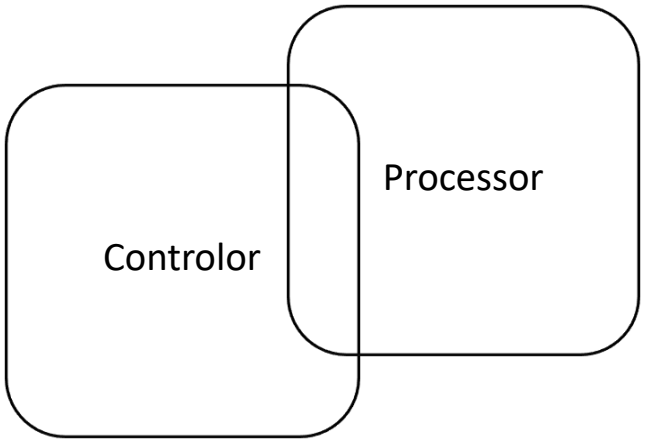
Who is the processor for whom?

In reality, frontiers can be blurred

Current issues related to companies' compliance with GDPR include contractual relationships with their IT solutions and services providers.

- When data is hosted in a SaaS solution, whose functionalities and technical characteristics are defined by the supplier, is the supplier still the processor of personal data?

- When a company physically hosts personal data but does not logically access it, is it a processor ?

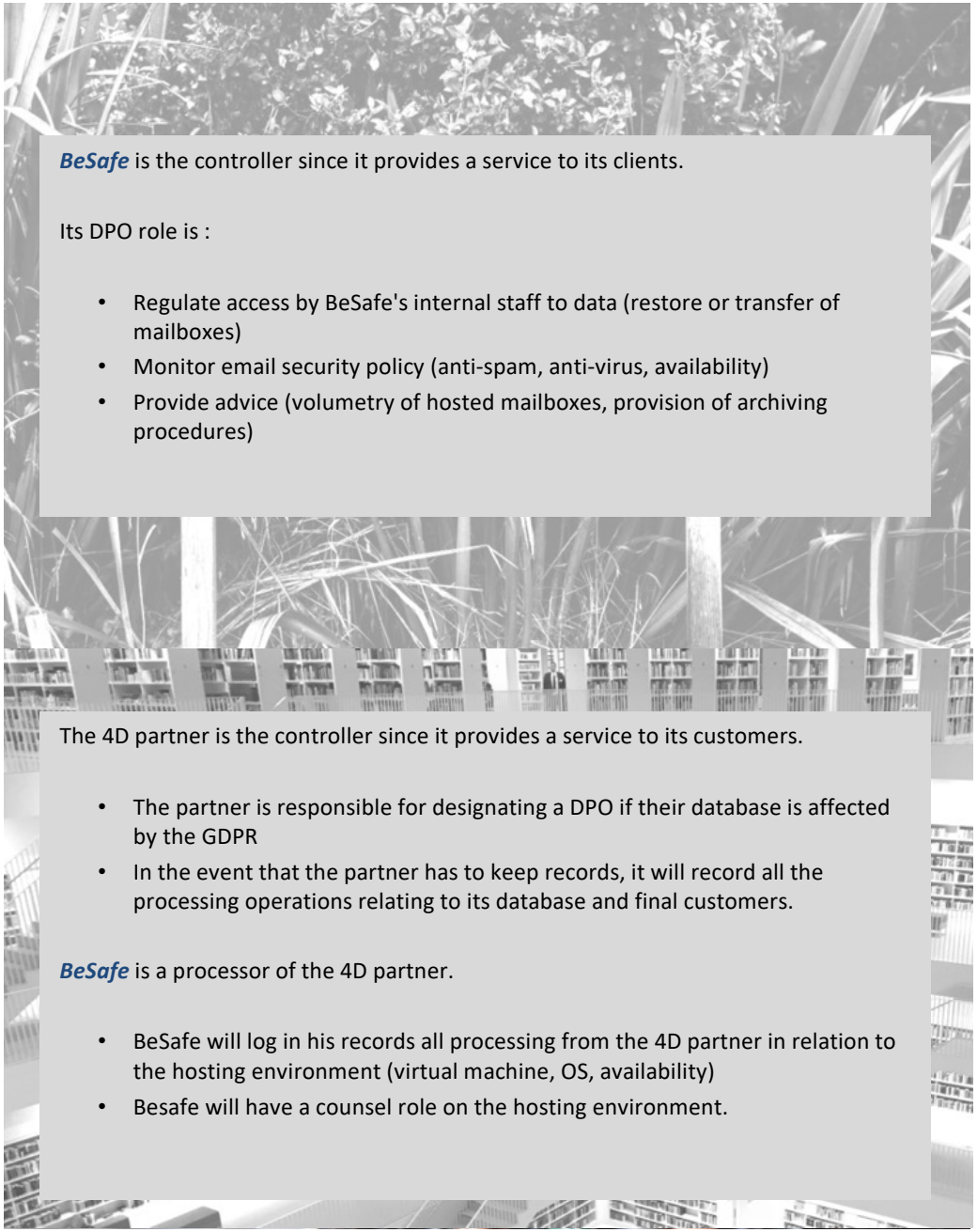


There is no answer with the GDPR

But…

In most cases, the host will be seen as the processor of a third party. Therefore, they must:

- Designate their own DPO;
- Keep records of internal treatments, with a record per client;
- Play the role of counsel with the hosted clients



BeSafe is the controller since it provides a service to its clients.

Its DPO role is :

- Regulate access by BeSafe's internal staff to data (restore or transfer of mailboxes)
- Monitor email security policy (anti-spam, anti-virus, availability)
- Provide advice (volumetry of hosted mailboxes, provision of archiving procedures)

The 4D partner is the controller since it provides a service to its customers.

- The partner is responsible for designating a DPO if their database is affected by the GDPR
- In the event that the partner has to keep records, it will record all the processing operations relating to its database and final customers.

BeSafe is a processor of the 4D partner.

- BeSafe will log in his records all processing from the 4D partner in relation to the hosting environment (virtual machine, OS, availability)
- Besafe will have a counsel role on the hosting environment.

Practice case

Case N°1 :

Besafe provides a private messaging service for one of its clients

- Hosting is internal to ***BeSafe*** without third party
- The messaging servers are located in France

Case N°2 :

Besafe hosts the virtual machine of a 4D partner who entrusts it with the administration of its system (outside of the database)

- Hosting is internal to ***BeSafe*** without a third party
- The messaging servers are located in France
- The ***BeSafe*** support does not have access to the content of the 4D base


10 GDPR criteria to evaluate your database

GDPR and database

The Data Storage

- The volume of database data
- Sensitivity of retained data
- The presence of identifying data

Examples

Will I still be able to record the names, email addresses, and mobile numbers of my business contacts in a database?

Yes, and under the same conditions as those of the current law: with the consent of the person concerned.

For the efficiency of B-to-B debt recovery, I often suggest that reminder officers write down information on the working hours of the representatives,

A distinction is made between working hours, which is personal data, and availability hours, which is professional data. So it's better to record the last ones.

GDPR and Database

Data Collection

- The volume of customer data added monthly

6% of audited parties comply with GRPD within six months of its entry into force.*

84% to 94% of websites do not ask for consent for the collection of personal data.*

* Source : Viuz.com

GDPR and Database

Data Transfer

- Transfer of data to third parties
- Data transfer outside the EU

Example

Does the fact that my customer or supplier databases are in the cloud, or hosted outside the European Union, change anything?

Not knowing where they are is already an indication of non-compliance. Personal data must be protected from intrusion under both the current law and GRPD, which strengthens sanctions.

GDPR and Database

Data Suppression

- Regular purging of irrelevant data
- Retention periods for personal data

deletion of an account after X months of inactivity, unsubscribe after X months without opening an email

GDPR and Database

Data Security

- Population with access to personal data
- Personal data protection rules


How to adapt your development
with GDPR

GDPR and development

Right of access

- If your web application is accessible to users, they must be able to modify their profile.
- Basic rule - all fields in your ‘users’ table should be editable via the user interface.
- Users must be able to correct all data concerning themselves, including data you have collected from other sources.

Consent check boxes

- For each particular processing activity, there must be a separate checkbox on the user profile.
- Ideally, these check boxes should come directly from the processing activity log.
- Note that check boxes should not be pre-selected as this does not count as "consent".

GDPR and development

Right to Forgetfulness

- Have a "forget me" method that takes a *'UserId'* and deletes all personal data about that user.
- Your users have profiles on your web application. You must give them a way to delete their profiles using this method.

Notify third parties of deletion

- All third parties to whom personal data has been transmitted. If transmitted to a cloud service (Salesforce, Hubspot, Twitter) call one of their APIs that allows deletion of personal data (manual process for Google).

Exporting data

- Have a method "export data". When you click on this option to export the data, the user must receive all the data you hold about them. Usually, this is at a minimum the data you delete with the "forget me" feature.

GDPR and development

See all my data

This function is very similar to that for exporting, except that the data must be displayed in the user profile.

- You must also tell the user how you process their data.
- You can simply print out all the records in your data process register for which the user has consented.

Keep data for longer than necessary

- If you have collected the data for a specific purpose, you must delete / anonymize it as soon as you no longer need it.
- Have a planned method to periodically browse and anonymize data (delete names and addresses).

BONUS: HOW TO PREPARE YOURSELF?

ACTION PLAN:

1. Mobilize resources internally (nominate a DPO if necessary)

2. List your treatments (in controller quality, in processor quality)

3. Audit / improve your software tools:

    a) Functional level;
    b) Technical and organizational measures;
    c) In terms of R&D;

4. Prepare/review documentation;

5. Prepare/review client communications;

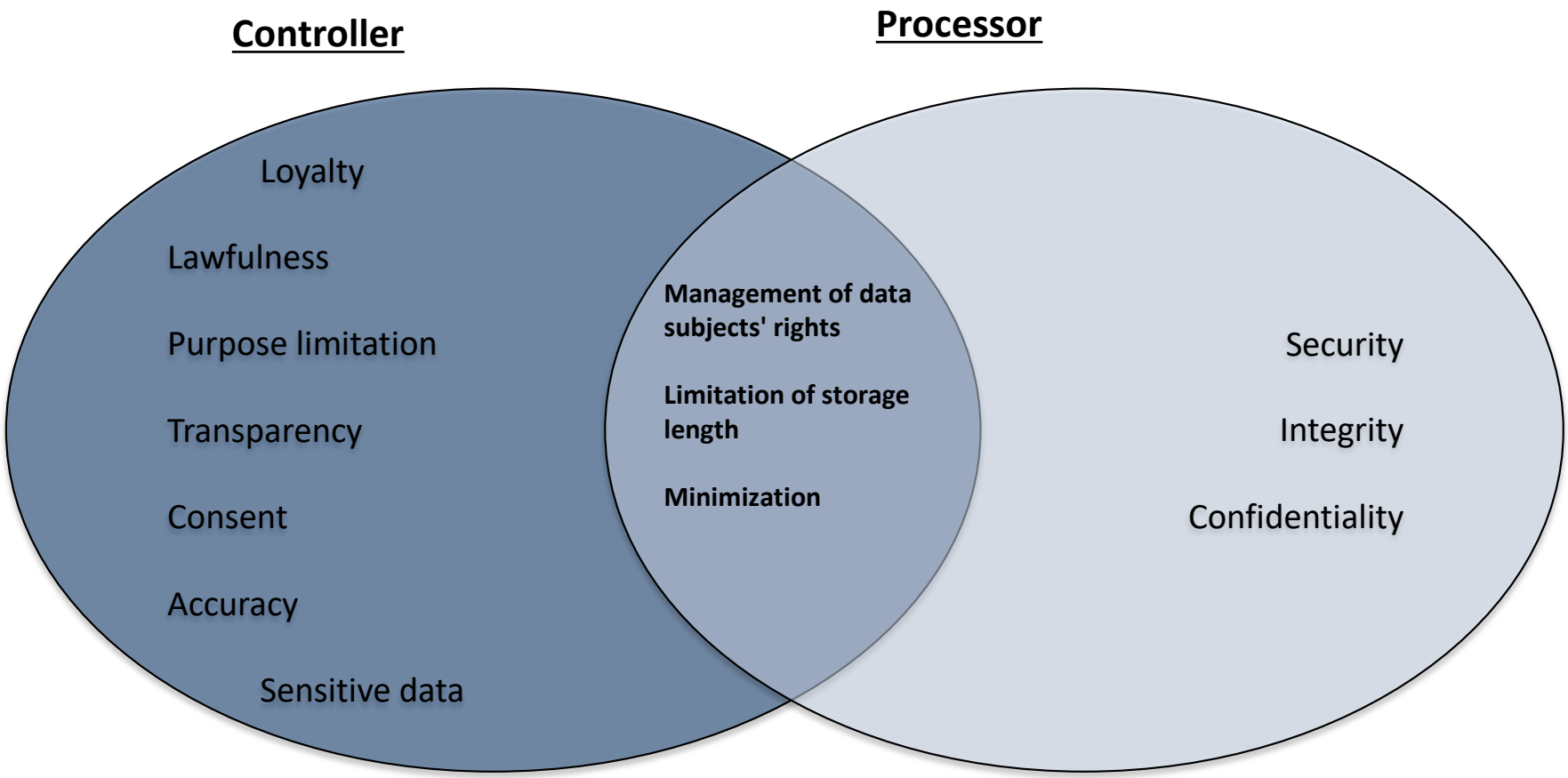
6. Review your existing contracts with your subsequent subcontractors;

7. Review your existing customer contracts;

8. Review your contract template with potential clients;

9. Position yourself on negotiated contracts based on the client's contract model.

The distribution of duties



BONUS: HOW TO PREPARE YOUR TOOLS?

Enabling Management and Access Control Policy

- Definition of authorization profiles and limitation of access by employees to the only data strictly necessary for the accomplishment of their missions
- Removal of users' access permissions as soon as they are no longer authorized
- Implementation of procedures systematically applied upon arrival, departure, or change of assignment of a authorized personnel.
- Annual review of authorizations

Event logging and record keeping policy

- Recording of relevant events
- Checking that logs cannot be changed
- Periodic review of event logs/systematic detection of anomalies
- Audit of procedures for immediate notification of any safety deficiencies/incidents

Encryption and hashing

- Adapted encryption solution
- Hash functions
- Pseudonymisation / anonymization
- Tools and measures to verify the integrity of the code

Security policy for workstations

- Firewall / Antivirus / Weekly software updates
- In-house data storage (regularly backed up storage space)
- Blocking of downloaded applications not coming from a trusted source
- Limiting the connection of moving media and disabling autorun

Data Backup Policy

- Periodically
- Backup servers (location, security measures in place, etc.)

Mobile Computing Security Policy

- Encryption of mobile phones
- Encryption of removable media
- Backup and synchronization mechanisms
- Theft protection mechanisms

BONUS : HOW TO PREPARE YOUR TOOLS?

Computer Network Protection Policy

- Blocking unnecessary services (ex: VoIP)
- Securing Wi-Fi networks (encryption)
- Partitioning of open networks / internal network guests
- Audit of access to user interfaces
- Limiting network flows to what is strictly necessary, filtering incoming and outgoing flows on equipment (firewall, proxy, servers, etc.)
- Verify that no administration interface is accessible directly from the internet

Server Security

- Access to the administration interface: strong authentication policy / enhanced access control
- Database Administration Policy
- Nominative accounts for access to databases
- Application-specific accounts for each application
- Measures against attacks by injection of SQL code, scripts, etc.
- Partitioning of sensitive data
- Server administration environment via a dedicated and isolated network
- Vulnerability detection tools

Office Space Protection Policy

- Access rules (ex: badges, visitor escort), differentiated according to zones and persons concerned (employees/external service providers/visitors)
- Control measures / traceability of access to premises
- Means of physical protection of computer equipment

Business Continuity and Recovery Plan

- Customer contacts in the event of a claim
- Third party stakeholders
- Procedure followed
- Bypass Solution / Recovery Procedure / Back-up Server
- Time limits
- Periodic BCP Tests

BONUS : HOW TO PREPARE YOURSELF?

Review your customer contracts and future sub-contracts