MAYOLY Taking your care to heart	Data Breach Management		
	Reference: **DJRC-DDSI-2025-02**	**Version:** V1.0	**Validation Date:** 28/02/2025

Issued by (Function/Name/Sign)	Date	Valid from	Signatures
Data Protection Officer / Karine Renault	28/02/2025	28/02/2025	Karine RENAULT Certified by yousign
Reviewed by (Function/Name/Sign)	Date	Replaces Doc.no/version	Signatures
Director DDSI / Julien Ragey	28 /02/2025	n.a.	Julien RAGEY Certified by yousign
VP Legal / Chi-Woon Won	28/02/2025		CHI WOON WON Certified by yousign
Approved by (Function/Name/Sign)	Date		Signatures
EVP Legal, Risks and Compliance / Christophe Hamon	28/02/2025		Christophe Hamon Certified by yousign

Contents

1 Objective 2

2 Scope 2

3 Responsibilities 2

4 Definition of personal data breach 3

5 Flow chart 5

6 Procedure 6

7 Versions History 7

8 Addendum 1: Examples of personal data breaches 8

9 Addendum 2: Examples of security incidents which are NOT personal data breaches 9

10 Addendum 3: How to evaluate the severity of the impact on the privacy of affected persons according to CNIL's PIA knowledge base 10

11 Addendum 4: List of abbreviations and definitions 12

12 Distribution 13

1 Objective

The objectives of this procedure are to:

- Ensure that MAYOLY and all affiliates of the organization (hereinafter 'MAYOLY') comply with 2016/679 General Data Protection Regulation ('EU GDPR') and local country data privacy laws where relevant in case a personal data breach occurs and MAYOLY becomes aware of it.
- Protect the data privacy of individuals, whose personal data MAYOLY or one of its sub-contractors is processing.

2 Scope

In scope:

- Personal data breaches as defined by EU GDPR
- All functions and individuals within MAYOLY, including external consultants
- Paper, oral, or electronic form of personal data breaches

MAOYLY France and all subsidiaries located in Europe will have to apply this procedure in order to comply with the GDPR requirements.
Subsidiaries located outside the EU will be assisted on a case-by-case basis by Mayoly in implementing this SOP.

Out of scope:

- All breaches of information that do not contain personal data, for example:
  - information security incidents that cannot cause a personal data breach
  - confidentiality breaches that do not contain personal data
  - serious breach of Good Practices in Pharmaceutical industry (GxP)
  - more general CAPA (Corrective and Preventive Actions) / non-conformance.

3 Responsibilities

All employees and external consultants of MAYOLY should have been trained to GDPR upon joining MAYOLY.

All MAYOLY personnel are responsible for following and complying with this procedure. They are responsible for identifying breaches of confidentiality by MAYOLY, sponsors, sub-contractors or other parties, and notifying the MAYOLY Data Protection Officer (DPO) within 4 hours after they become aware of a data breach.

Data Protection Officer (DPO): is a professional with expertise in the field of personal data protection. His or her mission is to ensure that the organization processes data in accordance with the rules of the GDPR and other applicable legislation. He/she acts as an independent advisor to raise awareness and provide guidance to the organization's stakeholders. In the event of a data breach, DPO will meet the GDPR obligations and, depending on the severity of the data breach, consult the DPC for an in-depth expertise.

Data Privacy Committee (DPC) Core: The main role of the Data Privacy Committee is to define the overall Data governance, to make strategic recommendations and data security across the Group. It includes representatives from different departments with Legal & Compliance, Data Protection Officer (DPO), Information system for the permanent members and designated as DPC "Core". Depending on the Data Breach severity (defined in this SOP), this DPC "Core" will be accountable for making decisions as required, based on the recommendation of the DPO. Other parties may be involved in addition to the DPC "Core" on a case-by-case basis. Such additional parties are designated as DPC "ad-hoc". It may include, without limitation, head of Pharmacovigilance, Quality, Human Resources, Sales & Marketing or a subsidiary's/ affiliate's local representative, etc. as relevant.

4 Definition of personal data breach

4.1 A **personal data breach** is broadly defined as a security incident that affects the confidentiality, the integrity or the availability of personal information, whether the breach be deliberate or the result of an accident. So, there will be a breach whenever any personal data are lost, destroyed, corrupted or disclosed; if someone accesses the data or passes them on without proper authorization; or if the data are made unavailable (permanently or temporarily or truncated) or accidentally lost or destroyed.

Addenda providing examples of data breaches (addendum 1) as well as incidents that do not qualify as data breaches (addendum 2).

4.2 Look at the **impact** for the private life of data subjects, not for your organization

When evaluating the severity of a personal data breach, MAYOLY will look at the impact on the private life of the data subjects.

The below scale can be used to estimate the severity of data breach.

4.3. Severity of a personal data breach (refer to addendum 3 to estimate the severity)

1. Negligible severity ('minor breach'): a breach that doesn't have any impact on the private life of any data subject.
   A typical example is a 'point to point' data breach (see Addendum 1, example number 6). In such case, MAYOLY just needs to contact the wrong recipient of the email and ask him/her to delete the email or the document received by mistake.

2. Limited severity: a breach with potential impact such as: a breach which could potentially harm the private life of some data subjects. The severity is limited if the number of data subjects impacted by the breach is low and/or the personal data leak is limited to few professional contact details for example (by default, sensitive personal data breach are excluded unless demonstrated otherwise), and the breach has a limited impact onto data privacy and freedom for data subjects. Notification to Data Protection Authority may or may not be relevant and would need to be documented to justify the limited impact conclusion.

3. Significant severity: a breach with a potential impact on the data subject and must be confirmed by an forensic analysis to assess the severity of the risk. The data breach could harm the privacy of the data subject(s).In that case, MAYOLY will need to notify the local Data

Protection Authority (DPA) and/or ask them for their opinion. In parallel, and depending on the results of the forensic analysis, it could be that no data subjects have been impacted.
A typical example is if an IT associate discovers that cyber criminals have placed an additional 'fake' screen on a public sales portal selling cosmetics to consumers: the company didn't receive any complaint from any clients that their credit card details were stolen, so IT needs to perform an inquiry and check if there is evidence of a data flow outside of the normal flow;

4. Maximum severity: a breach where clearly the private life of data subjects can be impacted and it is mandatory to notify the local Data Protection Authority (DPA), and it will probably be necessary to inform the data subjects.
This is the case for example if a PV supplier forgets by mistake Adverse Events Reports in a taxi, or if the laptop of that PV supplier employee is stolen and was not encrypted.

The severity level thus obtained may be raised or lowered by including additional factors:

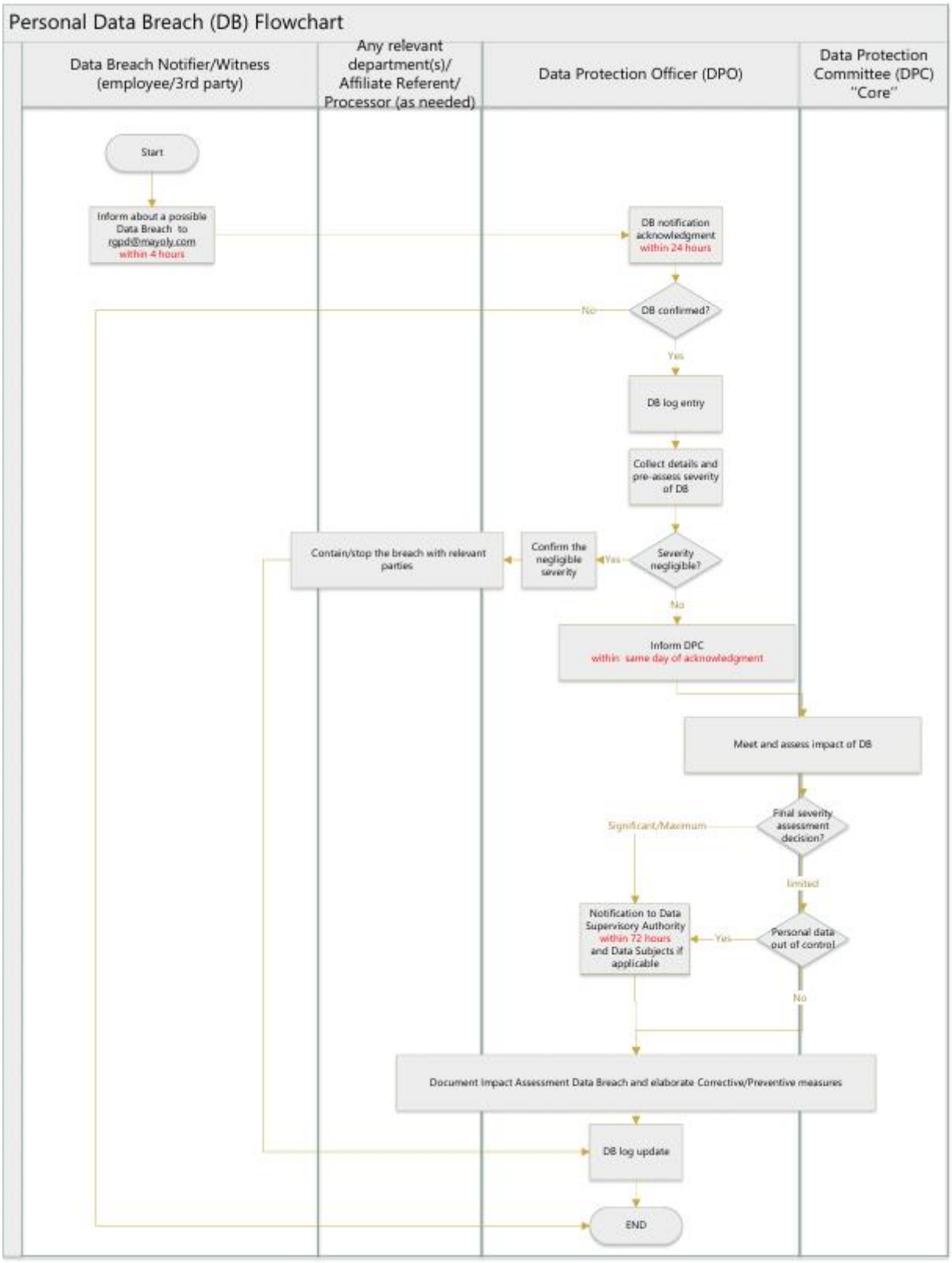
- level of identification of personal data;
- nature of risk sources;
- number of interconnections (especially with foreign sites);
- number of recipients (which facilitates the correlation between originally separated personal data).

In other words:

Severity of the data breach	Impact on the private life of the data subjects	DPC consultation	Notify local Data Protection Authority (DPA)?	Notify data subjects?	Notify police/cybercrime units?
Negligible	None or negligeable	No	No	No	No
Limited	Potential but limited	Possibly	May need to be notified case-by case	No	No
Significant	Potential, important and/or complex	Yes	Yes	No	No
Maximum	Yes	Yes	Yes	Probably yes, to discuss with DPA	Probably yes, to discuss with DPA

If the risks to data subjects are significant or maximum, then it is mandatory to notify the local Data Protection Authority. If you are unsure, the advice is to notify your local Data Protection Authority and ask them for directions.

5 Flow chart


Personal Data Breach (DB) Flowchart
Data Breach Notifier/Witness (employee/3rd party)
Any relevant department(s)/ Affiliate Referent/ Processor (as needed)
Data Protection Officer (DPO)
Data Protection Committee (DPC) "Core"
Start
Inform about a possible Data Breach to rgpd@mayoly.com within 4 hours
DB notification acknowledgment within 24 hours
DB confirmed?
No
Yes
DB log entry
Collect details and pre-assess severity of DB
Severity negligible?
Yes
Confirm the negligible severity
Contain/stop the breach with relevant parties
No
Inform DPC within same day of acknowledgment
Meet and assess impact of DB
Final severity assessment decision?
Significant/Maximum
limited
Personal data out of control
Yes
Notification to Data Supervisory Authority within 72 hours and Data Subjects if applicable
No
Document Impact Assessment Data Breach and elaborate Corrective/Preventive measures
DB log update
END

6 Procedure

Responsible	Step #	Description
1. Identification of a breach		
External notifier	1	Notifies a personal data breach (DB) to a MAYOLY employee. The external notifier is any person external to MAYOLY who becomes aware of a personal data breach for which MAYOLY is Data Controller or Processor.
Recipient of data breach	2	The receiver is the first MAYOLY employee who becomes aware of the breach: either receiver is notified by an external notifier (see step 1), or receiver detects the data breach by him/herself. On identifying, or being notified of, a personal data breach, • Informs within 4 hours the DPO by email at rgpd@mayoly.com (or by telephone, text message upon needs) • Informs his/her Line Manager for strict management acknowledgment (without transmitting any identifying data) Remark: In the event or suspicion of a cyber-attack scenario, please raise an IT Support ticket within 4 hours further investigation. • Provides as much information as possible about the potential breach. If it is a negligible 'point to point' breach (see section 4.3), receiver immediately asks the recipients who received the personal data in error to delete such data and email, and to confirm such deletion in writing.
2. Breach assessment and reporting		
DPO	3	a. Acknowledges the DB within 24 hours after breach receipt or identification by MAYOLY b. Based on information provided by the receiver or notifier evaluates if the DB is confirmed If the DB is confirmed: c. Completes the DB log d. Collects any useful information from the receiver and/or notifier to evaluate the DB severity. **If the DB is negligeable** (= with no impact on DS): e. the DPO confirms to the receiver of the breach or if doable quickly (e.g. if there is only one DS affected, and in most breaches where impact is negligible), contacts immediately the recipient(s) of personal data that it is negligible and checks the breached data has been deleted by the wrong recipient and same is confirmed in written. f. Completes/updates the DB log **If the breach is limited, significant or maximum severity** (see definitions above in section 4):

Responsible	Step #	Description
		g. the DPO informs Core DPC during same day of acknowledgment by email or any written mode with - summary of risk evaluation, breach details, and recommended action plan to DPC for decision; - in particular indicates if he/she thinks risk is not negligible and local DPA should be informed, and/or if DS should be informed and how. h. Completes/updates the DB log
Core DPC and any Relevant Representative (as appropriate)	4	Meets & evaluates the severity of impact on the privacy of affected persons according to the number of data subjects concerned, their type (children, senior people, etc.), the type of data (sensitive or not, directly identifying or not), the amount of data for each data subject. Also, CNIL's PIA knowledge base can be used (see in addendum 3). **If the breach is limited:** at least the DPC and DPO must assess the impact of the leak for making decision of Data Authority notification, - if the DB is out of control, please continue from step 5 below. - if not, notification to the DPA is not necessary. Please continue from step 6 below. **If the breach is significant or maximum,** please continue from step 5 below.
DPO	5	If instructed so by Core DPC, informs local DPA and/or DS; within 72 hours after breach receipt or identification by MAYOLY
3. Personal Data Breach documentation		
DPO	6	All the documentation related to data breach identification, follow-up, implemented Correction actions /preventive actions, exchange with local DPA if any, closure should be recorded to the shared drive secured made available and accessible by DPO and DPC.
4. Follow-up and Quarterly review of Personal Data breach		
DPO	7	Provides quarterly reports to DPC; the reports will summarize main GDPR events of the period and highlight the risk(s) incurred by MAYOLY during the past quarter or year and suggest CAPA if relevant.

7 Versions History

version	Date	Change history
1.0	*01/Feb/2024*	*Initial Version*

8 Addendum 1: Examples of personal data breaches

Examples of unauthorized disclosures breaches:

1. A pharmacist emails to MAYOLY the name and photography of a consumer regarding a drug quality complain.
2. A staff member copies an email to all HealthCare Professional invited to the next webinar without using the blind copy function (all email addresses can be seen by all volunteers).
3. A staff member sends to a third party a list of MAYOLY staff members' home telephone numbers.
4. MAYOLY's pension provider sends details of a staff member's pension to the wrong member of staff.
5. The finance department receives information containing payroll details of people who don't work at MAYOLY.
6. An employee sends an email containing personal information to the wrong recipient due to data entry error of email address in the email software (point to point).
7. A person sends by email to MAYOLY a document that he/she found in the metro: the document is from a clinical study with encoded patient health data on it and the name of the clinical site and of the healthcare professional: the above person says that he/she found the paper document on the floor in a train station.
8. One of MAYOLY vigilances' providers sends you some adverse events details with full name of consumer in clear text.
9. An HR employee forgets a paper document at the copy machine; this document contains the salary amounts of all employees of a department.
10. An employee of MAYOLY has been victim of a theft in subway. His private cell phone has been stolen. His cell phone allows an access to his MAYOLY's outlook.
11. One of a MAYOLY's third party provider lost a backup of MAYOLY's data that was used few days ago as part of a new software implementation.

Examples of data integrity loss:

12. One employee of MAYOLY is granted to a software application (E.g. Veeva CRM, ERP, Harmonica, etc…) with a wrong user profile access that will permitting him/her to change/modify/delete some records/personal data of other affiliates/departments out of scope of current user accountability/responsibility.
13. During a software migration some records are truncated, loss, changes when unplanned.
14. The software does not have any audit trail allowing to trace which record data has been changed by whom and by when.

Examples of data unavailability:

15. MAYOLY is the victim of a cyber-attack with ransomware. Data of all Healthcare Professional or HR records, or other records are no longueur displayed or lost due to database encryption.
16. One of software application is no longer available for several days due to a significant bug/malfunction causing no availability of data for some times.

9 Addendum 2: Examples of security incidents which are NOT personal data breaches

1. The paper document containing the pricing list of a supplier distributing your products is lost by that employee in a public area: as this pricing list doesn't contain any personal data, it is NOT a personal data breach; it has no impact on any specific person; in this case, it is a breach of confidentiality and of intellectual property for the supplier; the impact will be for the business of this supplier.
2. An employee working for a pharmaceutical company sends by mistake an email to a wrong recipient outside the organization; this email contains the list of the healthcare products sold by the company.
3. A thief accesses the headquarters during the night and steals several mobile phones; the phones do not contain any personal data as they were brand new and were unpacked.

10 Addendum 3: How to evaluate the severity of the impact on the privacy of affected persons according to CNIL's PIA knowledge base

Privacy Impact Assessment (PIA) – Knowledge bases – from CNIL February 2018 edition Paragraph 1.5. Scales and rules for estimating severity, page 9.

1.5. Scales and rules for estimating severity

Severity represents the magnitude of a risk. It is primarily estimated in terms of the extent of potential impacts on data subjects, taking account of existing, planned or additional controls (which should be mentioned as justification).

The following scale can be used to estimate the severity of feared events (**Important: these are only examples, which can be very different depending on the context**):

Levels	Generic description of impacts (direct and indirect)	Examples of physical impacts[3]	Examples of material impacts[4]	Examples of moral impacts[5]
1. Negligible	Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem	- Lack of adequate care for a dependent person (minor, person under guardianship) - Transient headaches	- Loss of time in repeating formalities or waiting for them to be fulfilled - Receipt of unsolicited mail (e.g. spams) - Reuse of data published on websites for the purpose of targeted advertising (information to social networks, reuse for paper mailing) - Targeted advertising for common consumer products	- Mere annoyance caused by information received or requested - Fear of losing control over one's data - Feeling of invasion of privacy without real or objective harm (e.g. commercial intrusion) - Loss of time in configuring one's data - Lack of respect for the freedom of online movement due to the denial of access to a commercial site (e.g. alcohol because of the wrong age)
2. Limited	Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties	- Minor physical ailments (e.g. minor illness due to disregard of contraindications) - Lack of care leading to a minor but real harm (e.g. disability) - Defamation resulting in physical or psychological retaliation	- Unanticipated payments (e.g. fines imposed erroneously), additional costs (e.g. bank charges, legal fees), payment defaults - Denial of access to administrative services or commercial services - Lost opportunities of comfort (i.e. cancellation of leisure, purchases, holiday, termination of an online account) - Missed career promotion - Blocked online services account (e.g. games, administration) - Receipt of unsolicited targeted mailings likely to damage the reputation of data subjects - Cost rise (e.g. increased insurance prices) - Non-updated data (e.g. position held previously)	- Refusal to continue using information systems (whistleblowing, social networks) - Minor but objective psychological ailments (defamation, reputation) - Relationship problems with personal or professional acquaintances (e.g. image, tarnished reputation, loss of recognition) - Feeling of invasion of privacy without irreversible damage - Intimidation on social networks

[3] Loss of amenity, disfigurement, or economic loss related to physical integrity.
[4] Loss incurred or lost revenue with respect to an individual's assets.
[5] Physical or emotional suffering, disfigurement or loss of amenity.

CNIL. 4

Levels	Generic description of impacts (direct and indirect)	Examples of physical impacts[3]	Examples of material impacts[4]	Examples of moral impacts[5]
			- Processing of incorrect data creating for example accounts malfunctions (bank, customers, with social organizations, etc.) - Targeted online advertising on a private aspect that the individual wanted to keep confidential (e.g. pregnancy advertising, drug treatment) - Inaccurate or inappropriate profiling	
3- Significant	Data subjects may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties	- Serious physical ailments causing long-term harm (e.g. worsening of health due to improper care, or disregard of contraindications) - Alteration of physical integrity for example following an assault, an accident at home, work, etc.	- Misappropriation of money not compensated - Non-temporary financial difficulties (e.g. obligation to take a loan) - Targeted, unique and non-recurring, lost opportunities (e.g. home loan, refusal of studies, internships or employment, examination ban) - Prohibition on the holding of bank accounts - Damage to property - Loss of housing - Loss of employment - Separation or divorce - Financial loss as a result of a fraud (e.g. after an attempted phishing) - Blocked abroad - Loss of customer data	- Serious psychological ailments (e.g. depression, development of a phobia) - Feeling of invasion of privacy with irreversible damage - Feeling of vulnerability after a summons to court - Feeling of violation of fundamental rights (e.g. discrimination, freedom of expression) - Victim of blackmailing - Cyberbullying and harassment
4- Maximum	Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome	- Long-term or permanent physical ailments (e.g. due to disregard of contraindications) - Death (e.g. murder, suicide, fatal accident) - Permanent impairment of physical integrity	- Financial risk - Substantial debts - Inability to work - Inability to relocate - Loss of evidence in the context of litigation - Loss of access to vital infrastructure (water, electricity)	- Long-term or permanent psychological ailments - Criminal penalty - Abduction - Loss of family ties - Inability to sue - Change of administrative status and/or loss of legal autonomy (guardianship)

The value of the level that best matches the potential impacts identified is then selected, by comparing the impacts identified in the context considered with the generic impacts in the scale.

The severity level thus obtained may be raised or lowered by including additional factors:

- level of identification of personal data;
- nature of risk sources;
- number of interconnections (especially with foreign sites);
- number of recipients (which facilitates the correlation between originally separated personal data).

CNIL. 5

11 Addendum 4: List of abbreviations and definitions

Terms/Abbreviations	Definitions
Affiliates	Any legal person that directly, or indirectly through one or more intermediaries, Controls, is Controlled by or is under common Control with such first legal person. "Control" means for the purpose of this definition (a) the power to direct the management or policies of a legal person, whether through ownership of voting securities or by contract relating to voting rights or corporate governance, resolution, regulation or otherwise, or (b) to own more than 50% of the outstanding voting securities or other ownership interest of such legal person. In the case of legal persons organized under the laws of certain countries, the maximum percentage ownership permitted by law for a foreign investor may be less than fifty percent (50%) and in such case such lower percentage shall be substituted in the preceding sentence, provided that such a foreign investor has the power to direct the management and policies of the legal person.
CAPA	Corrective and Preventive Action
CNIL	French local Data Protection Authority
CRA	Clinical Research Associate
CRF/eCRF	Case Report Form/electronic Case Report Form
CRO	Contract Research Organization
DB	Data Breach
Data Controller	MAYOLY and its affiliates which, alone or jointly with others, determine the purposes and means of the processing of personal data collected from Data Subjects
Data Processor	MAYOLY and its Affiliates which processes personal data on behalf of a Data Controller
DPA	Data Protection Authority
DPC	Data Protection Committee
DPO	Data Protection Officer
Data Subject (DS)	A person who can be identified or identifiable because their data are processed
EEA/	European Economic Area
EU	European Union
GDPR	General Data Protection Regulation EU 2016/679
GxP	GxP is the abbreviation of "Good x Practice". The "x" in GxP stands for the field the guidelines and regulations applied to. This includes Good Clinical Practices (GCP), Good Manufacturing Practices (GMP), Good Laboratory Practices (GLP), Good Distribution Practices (GDP) and Good Vigilances Practices (GVP).
UK	United Kingdom

12 Distribution

Registered electronic copies :

Fonction	Name	Number of copies
Comex, N-1, N-2	Every direction and Mayoly Department	1