

Data Breach Reporting Form

1. Employee Identification

Name	
Area	
Contact	
Function	

2. Incident Information:

Time/Date of violation onset	
Time/Date of violation end	
Time/Date of knowledge of the breach	
How you became aware of the violation	

Type of violation:	☐	Integrity (improper alteration)
	☐	Confidentiality (improper access or disclosure)
	☐	Availability (improper deletion)

Nature of violation:	☐	Lost or stolen equipment
	☐	Lost or stolen documents
	☐	Lost or improperly accessed mail
	☐	Hacking
	☐	Malware
	☐	Phishing
	☐	Other

Cause of violation:	☐	Non-malicious internal act
	☐	Malicious internal act
	☐	Non-malicious external act
	☐	Malicious external act
	☐	Other

Incident Description:

3. Consequences of violation:

Integrity

Can data alteration/corruption have consequences for data subjects? ☐ Yes ☐ No

Indicate which ones:

Can data alteration/corruption be reverted to its original state? ☐ Yes ☐ No

Was the data encrypted? ☐ Yes ☐ No

Confidentiality

Can data alteration/corruption have consequences for data subjects? ☐ Yes ☐ No

Indicate which ones:

Availability

Could the loss of data availability have resulted in consequences for the data subject (during the breach or in the future)? ☐ Yes ☐ No

Indicate which ones:

Additional notes:

4. Personal Data:

Types of personal data:	☐	Identification data (Name, ID, NIF)
	☐	Contact details (telephone, email, address)
	☐	Financial data
	☐	Sensitive data (e.g. health data)

Other data:

Is it possible to determine the number of subjects involved? ☐ Yes ☐ No

Number of subjects involved:

5. Data Subjects:

Holders of personal data	☐	Workers
	☐	Clients
	☐	Others

Additional notes:

6. Information for holders:

Were the holders informed of the breach? ☐ Yes ☐ No

Time/Date of violation report:

Form of communication of violation:

Number of holders contacted:

Message sent to the holders:

7. Preventive/Corrective Measures:

What measures were applied