Data Breach Risk Assessment – Introduction

⚠- *If you have **no or limited experience** in carrying out data breach risk assessment, please read the following excerpt*

- **What is a Personal Data Breach?**

A **personal data breach** is a "breach of security leading to the **accidental** or **unlawful** destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

- **What are the possible consequences of a personal data breach?**

The **possible consequences** of personal data breaches can include but are not limited to significant adverse effects on individuals, which can result in physical, material, or non-material damage such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned

- **What are the possible root causes of personal data breach?**

The root causes of a personal data breach can arise from a combination of **human, technical, organizational, and external** factors. Common causes include human error (such as misdirected emails, accidental disclosures, or handling of personal data circumventing the designated security measures), phishing and other social engineering attacks, weak authentication mechanisms and inadequate access controls, software vulnerabilities and unpatched systems, malware and ransomware infections, misconfigurations of systems or cloud services, insider threats (whether malicious or negligent), inadequate security monitoring, third-party or supplier failures, loss or theft of devices or documents, insufficient security policies and procedures, and physical security incidents. External factors such as cyberattacks, exploitation of zero-day vulnerabilities, or other malicious activities may also contribute to a breach.

- **What is a personal data-breach risk assessment?**

A personal data breach risk assessment is the structured evaluation to determine the level of probability, the potential consequences and their severity to the fundamental rights and freedoms of the impacted individuals, following a breach involving their personal data. This assessment, in the context of the EUDPR, would result into one of three tiers: **unlikely risk**, **risk** and **high risk** to support consistent decision making on appropriate measures to mitigate those risks.

- **What are the elements to keep in mind when conducting a data breach risk assessment?**

A personal data breach assessment should be conducted **promptly** (upon awareness), to ensure that appropriate measures are implemented to protect the affected individuals. Keep in mind that the future **likelihood and impact** of harm occurring to an individual should be at the center of the risk assessment and the factual information on the breach should be used as a basis for such assessment. There may be a need to perform different **iterations** of the assessment whenever new information becomes available, to ensure that decisions on mitigating measures and notification decisions remain

appropriate and based on the most accurate and up-to-date information. For example, as an investigation progresses, additional facts may change the understanding of the breach, including its scope, root cause, affected individuals, or potential impact.The perception of a risk can differs among different people; for this the risk assessment needs to be as objective and as transparent as possible (by explaining the different factors that led to it).

The risk assessment method can be qualitative and should take into account several factors, among which the type of the breach, the nature, sensitivity and volume of personal data, the special characteristics of the affected individuals and the severity of consequences of the affected individuals. The context of the processing is important in understanding the risks to individuals and could introduce several other factors, including reasons to aggravate or decrease the risk assessment result. So, an understanding of the data processing and its context is a prerequisite to enable an informed risk assessment.

	What to Assess	***Aggravating factors examples***	***Mitigating Factos (Examples)***
Data characteristics	Type, sensitivity and volume of personal data affected. Context of processing.	Sensitive data related to health, large volume of data . Output of processing	Pseudonymized data, basic identifiers
Category of data subject	What is the relationship between the individual and their data, whether they are part of a vulnerable group	Children, politicians etc... Context of data can reveal sexual orientation/ health status	No vulnerable groups
Nature of breach	Which part of the "CIA" did the breach effect? Confidentiality? Integrity? Availability?	Threat actor specifically targeting the individuals or the personal data to use for other non legitimate purposes	Known recipient of data with contractual obligations of secrecy. Exposure was for a limited time with no effect of CIA
Likelihood and severity of harm	Potential future impacts	Data is on the dark web	Probability of harm is significantly low in the given context
Mitigation measures	What mitigation measures were taken before and after the breach to secure the data	Unauthorized communication channel used in professional context, lack of MFA technology	Log monitoring, recommendation to data subjects on prevention of harm

Please note: This table is provided for illustrative purposes only and highlights examples of circumstances that may influence a data breach risk assessment. It is not intended to be an exhaustive list of all factors that should be considered.

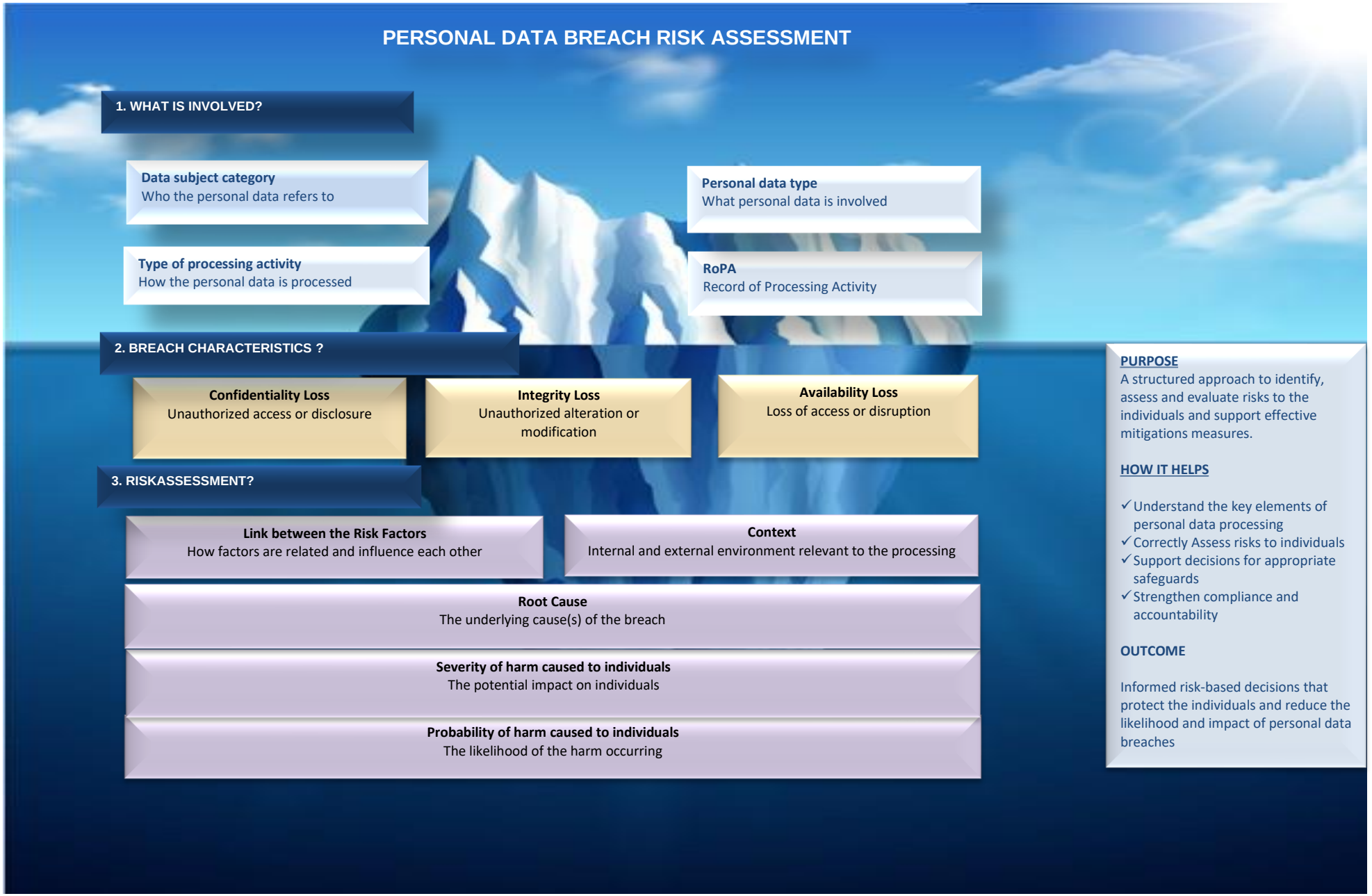
- ## Outcome of the risk assessment

As mentioned above, the main outcome of the risk assessment of a data breach is a list of identified risks for the affected individuals. Based on those risks, the controller can take decisions on the most appropriate measures to mitigate those risks. Sometimes there are no measures that can adequately mitigate the risks to the individuals. In this case, informing them of what happened and on the risks they are exposed to, can allow them to protect themselves (e.g. in cases of fraud).

Apart from the assessment of the risks to data subjects stemming from the particular personal data breach, you should work towards implementing a combination of organizational, technical, and physical security measures, to prevent the recurrence of a personal data breach and minimize its potential impact. These measures should address the root causes identified during the data breach investigations and strengthen the overall security posture of the organization.

⚠ Note

Please refer to the Reference library on the ARETE training dashboard for further readings. For additional information on Data Breach Risk Assessment, please consult the EDPB Guidelines.


PERSONAL DATA BREACH RISK ASSESSMENT
1. WHAT IS INVOLVED?
Data subject category
Who the personal data refers to
Personal data type
What personal data is involved
Type of processing activity
How the personal data is processed
RoPA
Record of Processing Activity
2. BREACH CHARACTERISTICS ?
Confidentiality Loss
Unauthorized access or disclosure
Integrity Loss
Unauthorized alteration or modification
Availability Loss
Loss of access or disruption
3. RISKASSESSMENT?
Link between the Risk Factors
How factors are related and influence each other
Context
Internal and external environment relevant to the processing
Root Cause
The underlying cause(s) of the breach
Severity of harm caused to individuals
The potential impact on individuals
Probability of harm caused to individuals
The likelihood of the harm occurring
PURPOSE
A structured approach to identify, assess and evaluate risks to the individuals and support effective mitigations measures.
HOW IT HELPS
✓Understand the key elements of personal data processing
✓Correctly Assess risks to individuals
✓Support decisions for appropriate safeguards
✓Strengthen compliance and accountability
OUTCOME
Informed risk-based decisions that protect the individuals and reduce the likelihood and impact of personal data breaches