Workshop on Data Protection in International Organizations

Co-hosted by the European Data Protection Supervisor and the UN World Food Programme

12 – 13 May 2022

Practical Approach to Data Breach Response

- [redacted]
- [redacted] ICRC
- [redacted] WFP

Moderator: [redacted] UNHCR

WFP World Food Programme

EDPS

[redacted]

Personal Data Breach Management for International Organisations

Introduction

- Personal data breach obligations vary depending on whether the International Organisation (IO) is granted Privileges and Immunities, has its own data protection framework or is subject to specific privacy regulations (e.g., GDPR)

- In any case, the IO must have a tailored and effective Data Breach Management Policies and Procedures in order to minimize the risk/harm for individuals, assure business continuity and safeguard the IO's reputation

- Today we will discuss Data Breach Management under GDPR, but the reflections can be applied *mutatis mutandis* to other cases

[redacted]

"Personal Data Breach"

EXECUTIVE EDUCATION RESEARCH & TRAINING

A **personal data breach** can be defined as "*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*" – Art. 4(12) GDPR

The GDPR, under the principle of **Accountability**, holds data controllers responsible for notifying supervisory authorities when a data breach occurs, unless it is unlikely to result in a risk to the rights and freedoms of natural persons. In more serious cases, data controllers may have to communicate the personal data breach directly to the affected data subjects.

[redacted]

Categories of Personal Data Breaches

EXECUTIVE EDUCATION RESEARCH & TRAINING

Personal data breaches can be categorised into 3 major groups:

1. Confidentiality breaches

- Where there is an unauthorised or accidental disclosure of, or access to, personal data.

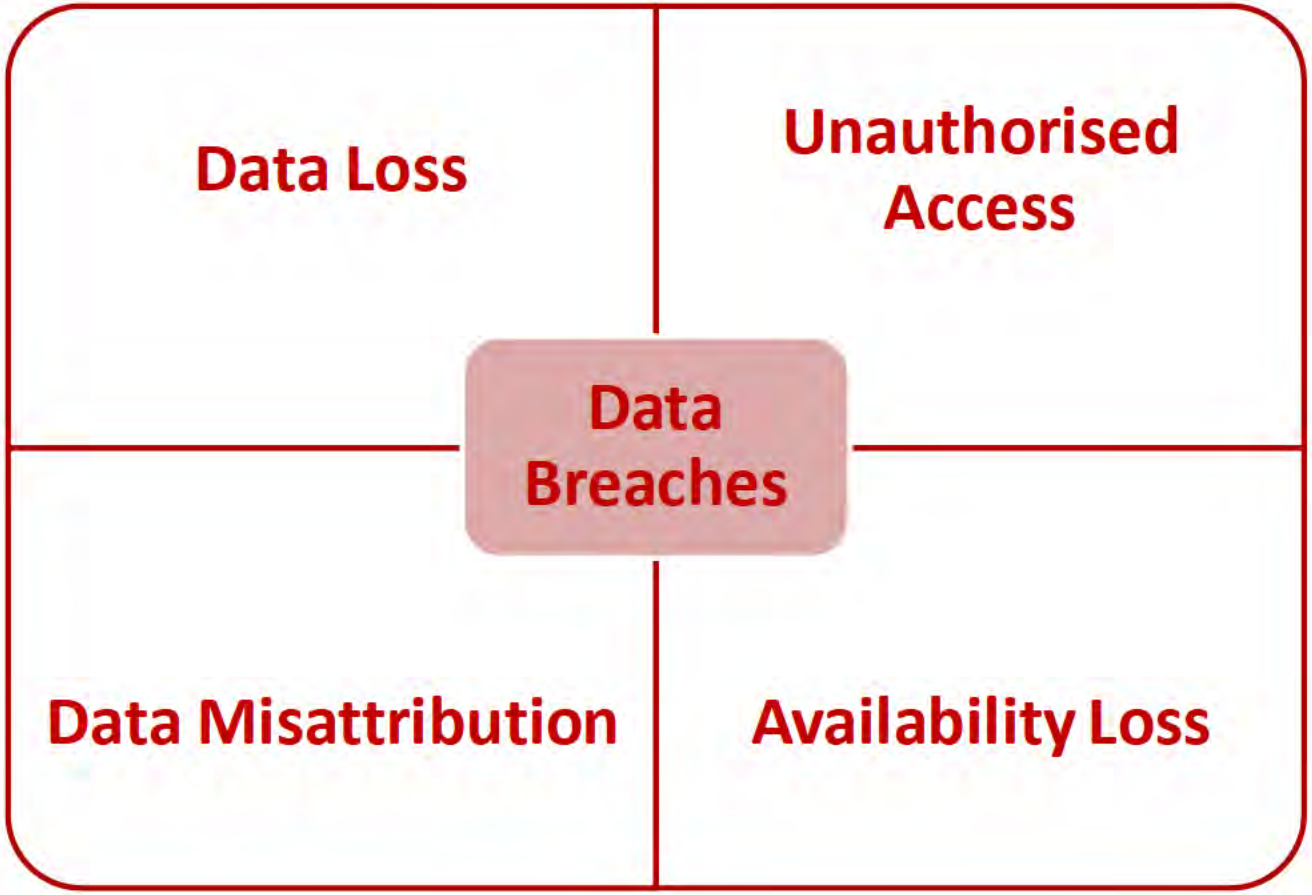
2. Availability breaches

- Where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

3. Integrity breaches

- Where there is an unauthorised or accidental alteration of personal data.

Examples of typical Personal Data Breaches



[redacted]

GDPR and Personal Data Breach Management

Notification to Supervisory Authorities

EXECUTIVE EDUCATION RESEARCH & TRAINING

Data controllers must notify personal data breaches to supervisory authorities without delay, and no later than 72 hours after becoming aware of one, as a rule.

Failure to notify a personal data breach, or to notify within 72 hours, may lead to corrective actions / orders and fines of up to EUR 10.000.000,00 (ten million euros) or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Data controllers are only exempted from this obligation where the personal data breach is "*unlikely to result in a risk to the rights and freedoms of natural persons*" – Art. 33(1) GDPR.

[redacted]

GDPR and Personal Data Breach Management

Communication to Affected Data Subjects

EXECUTIVE EDUCATION RESEARCH & TRAINING

If a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, it must also be communicated to the affected data subjects without delay.

Supervisory Authorities may require a data controller to carry out this communication, where they consider that this likelihood exists.

The data controller can be exempted from this obligation if:

- Appropriate security measures have been applied to the affected data (e.g., effective encryption);
- Other measures have been take to ensure the high risk has been contained (e.g., confirming deletion of unauthorised copies of personal data disclosed); **OR**
- This would involve a disproportionate effort – replaced by public communication or equally effective alternative.

[redacted]

Data Breach Severity Assessment

EXECUTIVE EDUCATION RESEARCH & TRAINING

The degree of risk that a personal data breach presents to the rights and freedoms of natural persons ("**severity**") is the trigger for notification/communication obligations under the GDPR.

Absence of GDPR-prescribed severity assessment methodology – useful to refer to relevant standards for an authoritative/tested approach.

ENISA's **Recommendations for a methodology of the assessment of severity of personal data breaches**
https://www.enisa.europa.eu/publications/dbn-severity

Severity Assessment (built on ENISA's standard)

EXECUTIVE EDUCATION RESEARCH & TRAINING

Breach Classification and Description

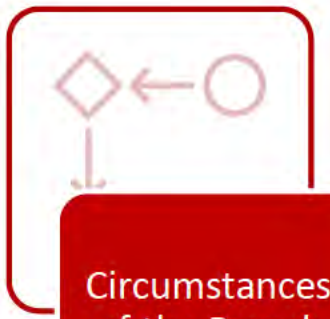
- Assign an identifier to the incident (e.g., "event code");
- Identify the category/type of breach (e.g., confidentiality, unlawful access);
- Provide a summary description of the facts concerned.

Data Processing Context (DPC)

- Assess the types of personal data affected (simple, behavioural, financial and/or sensitive);
- Assign score (**1-4**) based on context of the incident (e.g., volume of data, possibility for dangerous data reuse, vulnerability of data subjects).

Ease of Identification (EI)

- Assign score (**0,25-1**) based on the types of personal data affected (number of relevant identifiers, information available to potential recipients, degree of encryption / pseudonymisation).



Circumstances of the Breach (CB)

- Depending on the type of breach, assign score (**0-2**) based on additional aggravating circumstances (e.g., data disclosure to unknown number of recipients, impossibility to recover altered/lost data, malicious intent).

Overall Severity Assessment

Severity = (DPC x EI) + CB

- Severity < 2: **Low**;
- 2 ≤ Severity < 3: **Medium**;
- 3 ≤ Severity < 4: **High**;
- 4 ≤ Severity: **Very High**.

[redacted]

Severity explained

EXECUTIVE EDUCATION RESEARCH & TRAINING

Score	Level	Description
Severity < 2	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2 ≤ Severity < 3	Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ Severity < 4	High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
4 ≤ Severity	Very High	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.)

Managing a Personal Data Breach in Practice

EXECUTIVE EDUCATION RESEARCH & TRAINING

[redacted]

Phase 1: Gathering of Information

EXECUTIVE EDUCATION RESEARCH & TRAINING

- Information may be collected from internal channels (e.g., staff members) or external channels (e.g., data subject complaints, reports from third parties).
- Goal is to gather all relevant details regarding an incident and centralize them in a team responsible for assessing it.

Data Breach Assessment Unit (DBAU)

- Responsible for managing all incident reports and assessing whether they should be qualified as a personal data breach or not (**Phase 2**);
- May include an organisation's DPO, as well as members of the organisation's Legal, Privacy, Compliance, IT, Security or other functions.

[redacted]

Phase 2: Assessment

- **First-level:** Is this a security incident? Was the confidentiality, integrity and/or availability of personal data actually affected?

False positive.
(Skip to Step 4!)

Personal Data Breach.

- **Second-level:**

Data Breach Management Unit (DBMU)

- Responsible for jointly analysing all information collected and carrying out a more thorough **Data Breach Severity Assessment**, in order to appropriately assess its impact and comply with any associated obligations (**Phase 3**).
- Should include an organisation's DPO, as well as members of the organisation's Legal, Privacy, Compliance, IT, Security and other functions affected by the incident, as well as the organisation's management.

Phase 3: Notification / Communication

EXECUTIVE EDUCATION RESEARCH & TRAINING

Dependent on results of **Data Breach Severity Assessment**:

Low

- No need for notification/communication;

Medium

- Must be notified to competent Supervisory Authority, unless mitigating circumstances apply;
- Notification within 72 hours of awareness, in line with Art. 33 GDPR;

High & Very High

- Must be notified to competent Supervisory Authority (within 72 hours of awareness, in line with Art. 33 GDPR);
- Must be communicated to affected data subjects (without undue delay, in line with Art. 34 GDPR – directly or via public communication);

Phase 4: Recording

EXECUTIVE EDUCATION RESEARCH & TRAINING

All incidents assessed by the **DBAU** (including false positives) should be recorded in a **Register of Personal Data Breaches**.

- Meant to allow an organisation to demonstrate its compliance with its obligations under Arts. 33 and 34 GDPR, as well as to keep track of incidents to ensure they are appropriately addressed.

- A relevant owner for the **Register** should be identified (e.g., DPO, Compliance team, Legal team), who will be in charge of ensuring it is available and kept up-to-date.

- Information to be included (at least):
  - Incident identifier;
  - False positive or personal data breach;
  - Description of incident and consequences;
  - Description of measures taken to contain the breach and mitigate its impact;
  - Notification to competent Supervisory Authority (Y/N, date);
  - Communication to affected data subjects (Y/N, date);
  - Link to the corresponding **Data Breach Severity Assessment** (if available).

[redacted]

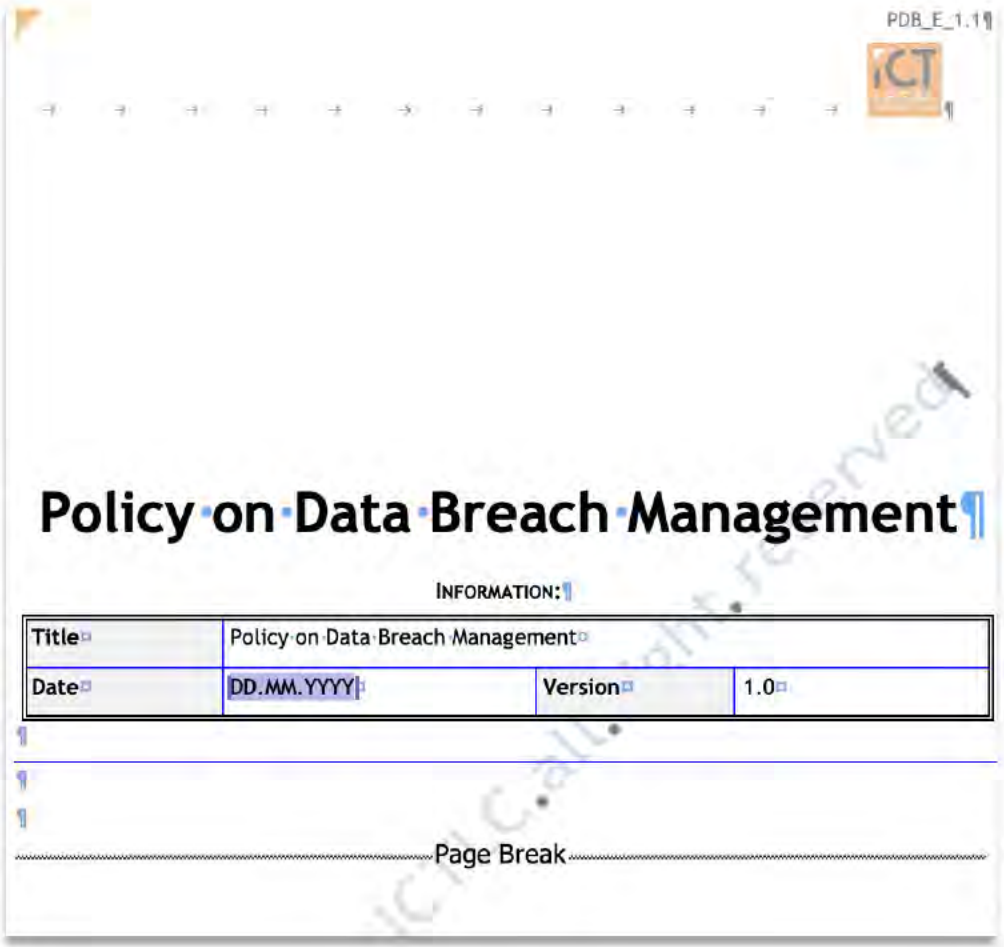
Phase 5: Post-Breach Analysis

EXECUTIVE EDUCATION RESEARCH & TRAINING

- Final collection of evidence/other information concerning the breach to be performed – ensure a complete root cause analysis of the incident has been carried out.
- Identify, on the basis of the root cause analysis, specific preventative measures which can be implemented to mitigate the risk of incident recurrence.
- Assess the effectiveness and efficiency of the procedure and the different teams involved in managing the incident, and identify possible areas of improvement.

[redacted]

Example of Policy on Data Breach Management



PDB_E_1.1¶

ICT

Policy on Data Breach Management¶

INFORMATION:¶

Title	Policy on Data Breach Management		
Date	DD.MM.YYYY	Version	1.0

¶

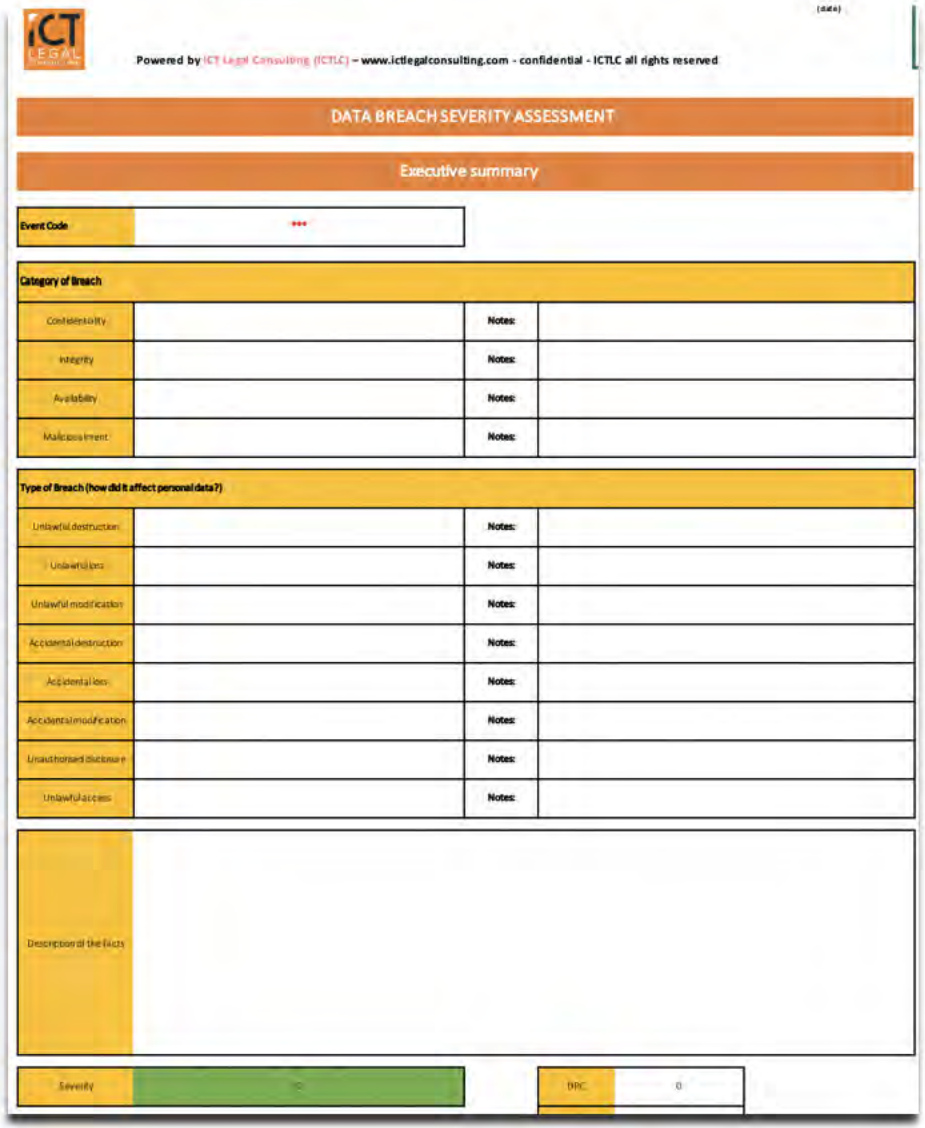
¶

¶

Page Break

[redacted]

Example of Data Breach Severity Assessment



Powered by ICT Legal Consulting (ICTLC) – www.ictlegalconsulting.com - confidential - ICTLC all rights reserved

DATA BREACH SEVERITY ASSESSMENT

Executive summary

Event Code	***

Category of Breach			
Confidentiality		Notes:	
Integrity		Notes:	
Availability		Notes:	
Malicious intent		Notes:	

Type of Breach (how did it affect personal data?)			
Unlawful destruction		Notes:	
Unlawful loss		Notes:	
Unlawful modification		Notes:	
Accidental destruction		Notes:	
Accidental loss		Notes:	
Accidental modification		Notes:	
Unauthorised disclosure		Notes:	
Unlawful access		Notes:	

Description of the facts			
Severity		DPC	0

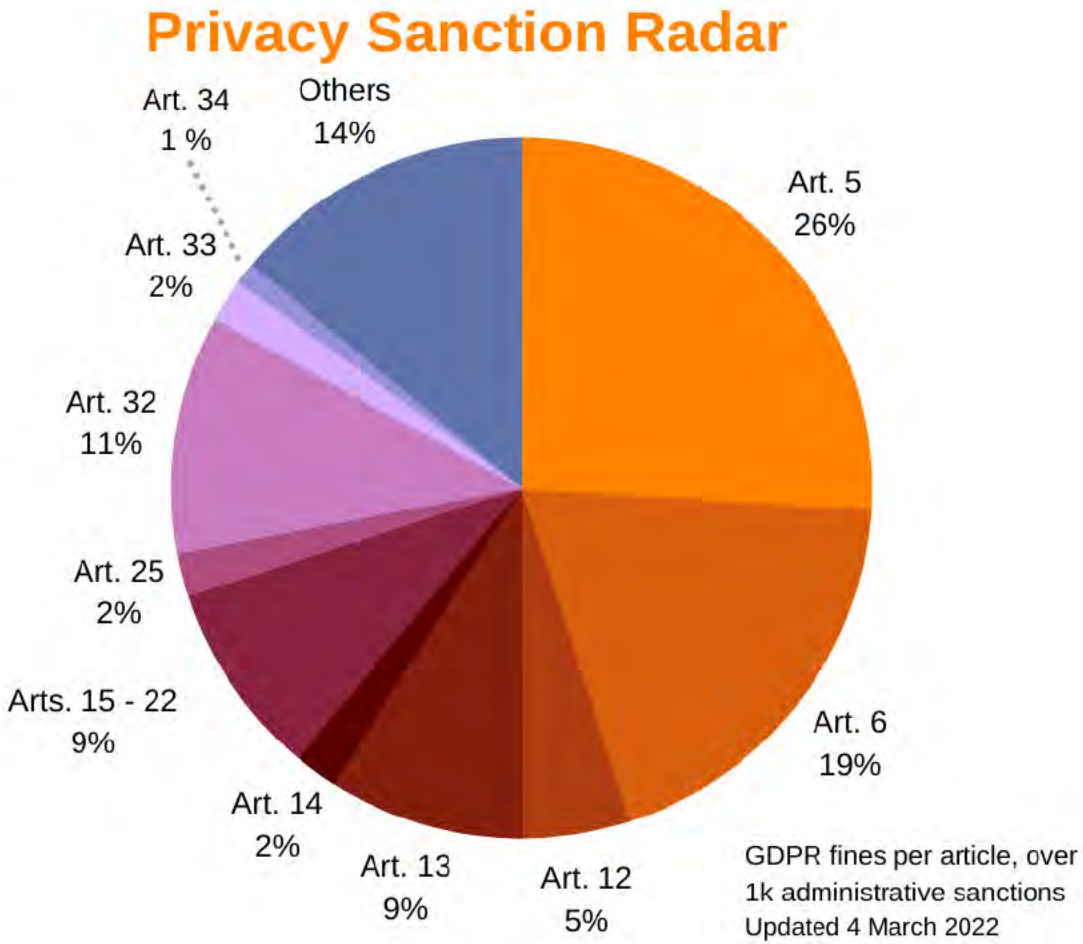
EXECUTIVE EDUCATION RESEARCH & TRAINING

Analysis of Sanctions Under the GDPR

EXECUTIVE EDUCATION RESEARCH & TRAINING

Based on the analysis of more than 1k enforcement actions, the majority of administrative fines to date *(some of which are combined, e.g., violation of Arts. 6 and 17)*, appear to show a concentration of violations of Articles **5, 6** and **32 GDPR**.

A significant number of sanctions have been issued for violations of Art. 32 GDPR (11%). Very often, EU DPAs are triggered to carry out an investigation following a data breach notification. Inspections frequently result in the DPA finding a lack of adequate security measures, leading to fines for Art. 32.



Interested in knowing more?

The [redacted] Case Law Observatory keeps track of all sanctions issued under the GDPR.

To receive a copy of [redacted]
"A sample of European Data Protection Authority 'Case Law' from 2018-2022: Article 5(1)(f) GDPR, Article 32 GDPR, Article 33 GDPR, Article 34 GDPR" booklet, write to [redacted]

[redacted]

EXECUTIVE
EDUCATION
RESEARCH &
TRAINING

Thank You!

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

EXECUTIVE
EDUCATION
RESEARCH &
TRAINING

[redacted]

[redacted]

ICRC

ICRC Central Tracing Agency Hack January 2022

EDPS WFP Workshop on Data Protection Within International Organisations. 12.05.2022

Pristina, Kosovo.* Fresh flowers attached to photographs of people who have been missing since the war ended in 1999.

ICRC

The hack

- Central Tracing Agency systems
- Hosting Re-establishment of Family Links data
- From a number of National Societies partners
- A sophisticated and targeted cyber operation

ICRC

Challenges and Lessons Learned

- Crisis Management
- Transparency

  Balancing act to maintain Neutral, Independent and Impartial Humanitarian Action
- Data Protection by Design in crisis situations

  Inclusion of DP legal advisors in the process

  Expedite DPIAs and processes, while developing higher standards

ICRC

Challenges and Lessons Learned

Protection of the affected population as a priority in diverse frameworks

- CTA network
  - Joint controllership
  - Clarification of roles and responsibilities
- Assessment of the Impact on the data subjects
  - Dialogue with partner National Societies
  - Diverse thresholds

ICRC

Challenges and Lessons Learned

Protection of the affected population as a priority in diverse frameworks

- Notification to Data Subjects

  Information mechanisms and preventing further risk

  Particularly vulnerable or high risks beneficiaries.

ICRC

Next Steps

- Information Security and Personal data protection reviews
- Best practices on risk assessment and notification processes
- Reinforce the protection and safety of the data, digital tools and infrastructures necessary to carry out humanitarian activities and mandate

ICRC

Many thanks for your attention !

[redacted]

ICRC

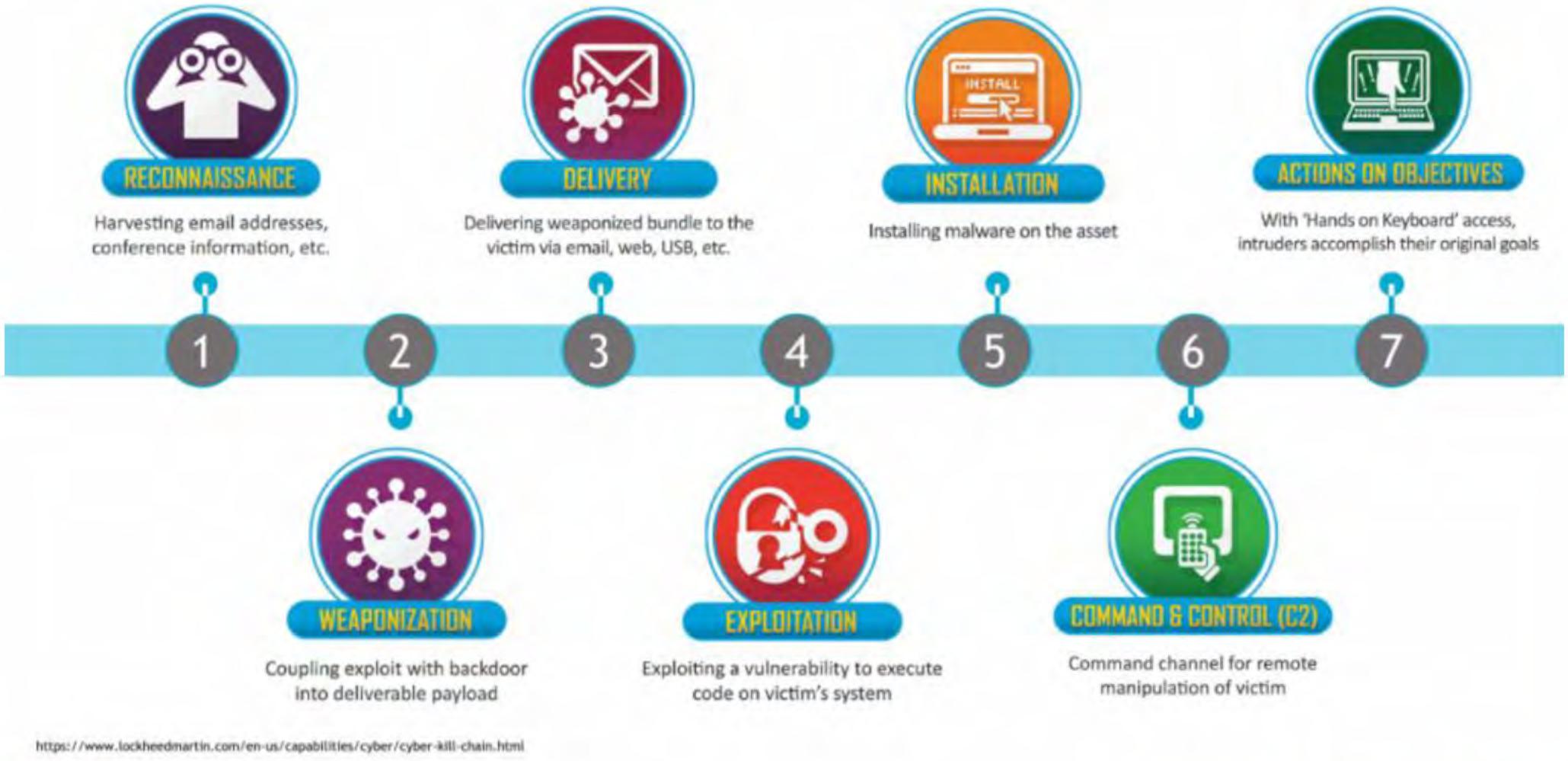
[redacted]

WFP

The CIA Triad

The CIA triad is a common model that forms the basis for the development of security systems and policies.


HIGH
MEDIUM
LOW
RISK

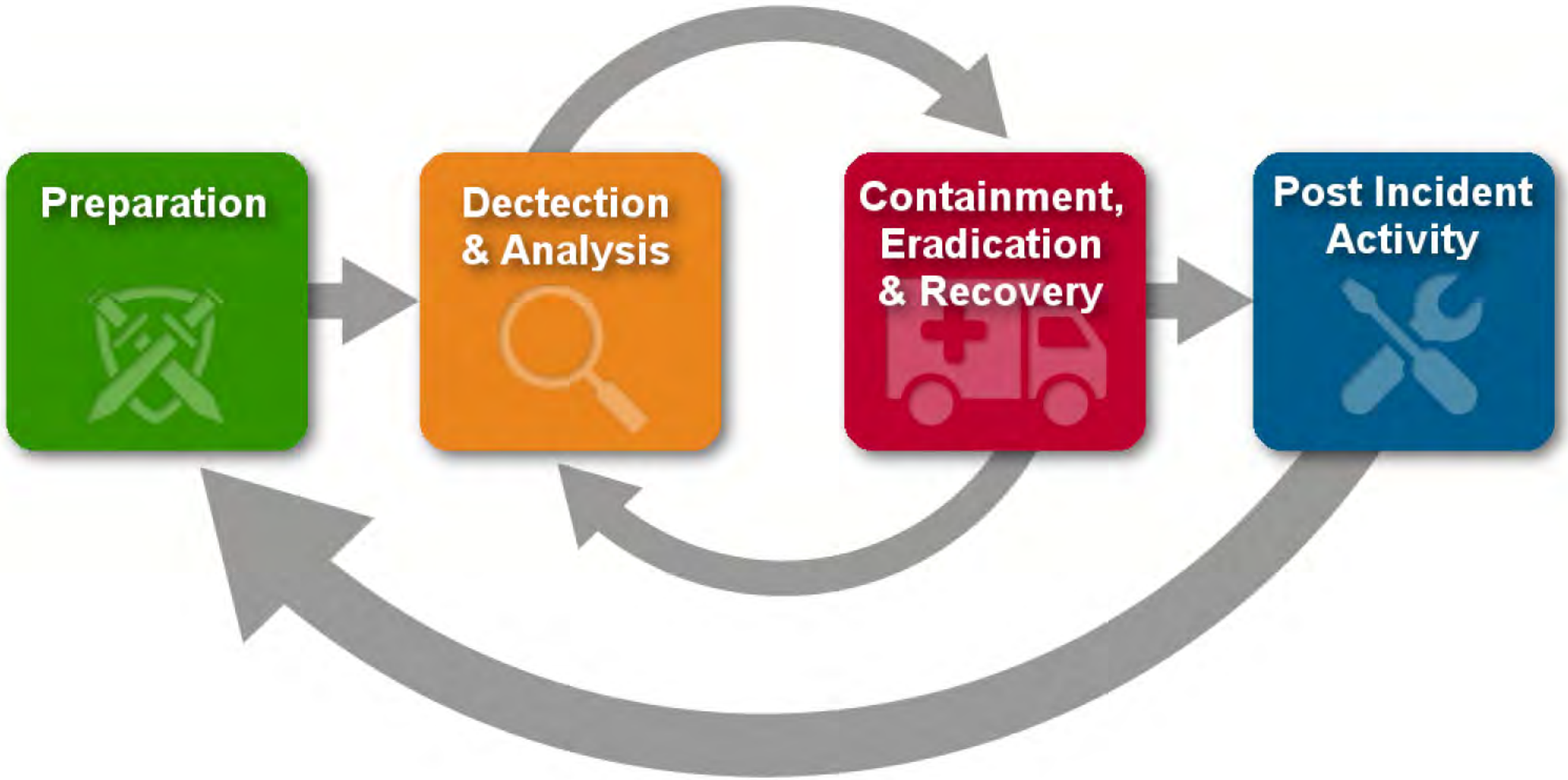


https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

WFP World Food Programme

Cyber Kill Chain

Incident Management Processes



Sample CIRT

- **Technology Division** shall be responsible for the management, update and overall execution of the CIRP;
- **Global Privacy Office** shall advise on risks for the individuals whose information is affected by the IT Security Incident;
- **Legal** shall advise over any legal implication or risk deriving from the specific type of Security Incident and over legal matters concerning post Security Incident activities;
- **Audit Office of Investigations** shall be informed of any action which may be subject to subsequent investigation;
- **Enterprise Risk Management** shall advice on risk assessment.

Who else?

- Communications?
- Program?
- Law Enforcement?

WFP World Food Programme