

CIRCL

Computer Incident
Response Center
Luxembourg

INFORMATION SHARING AND GDPR: A PRACTICAL PERSPECTIVE FOR CSIRTs

CIRCL C3 workshop

May 7th 2018

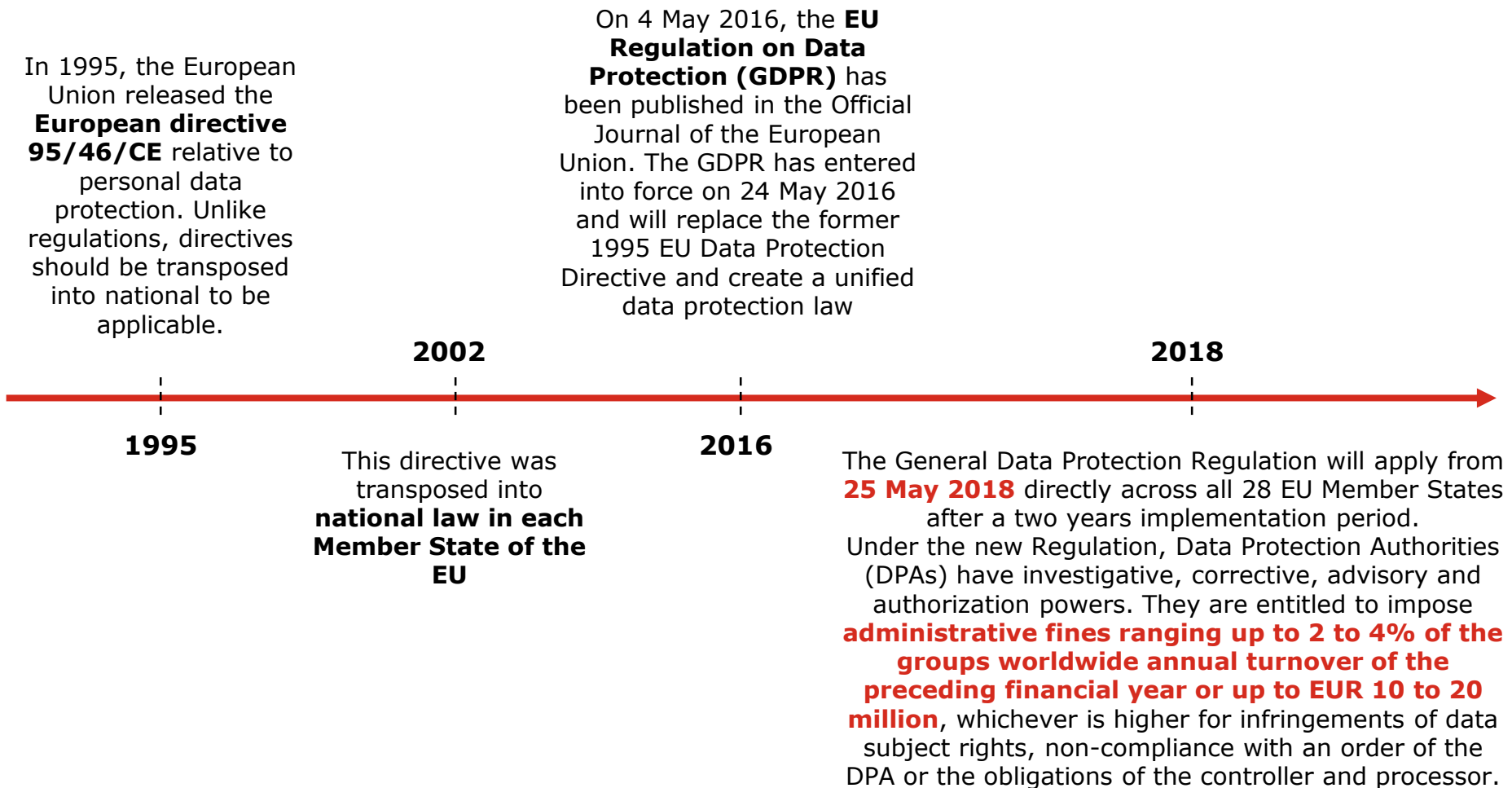


Co-financed by the European Union
Connecting Europe Facility

GDPR refresh

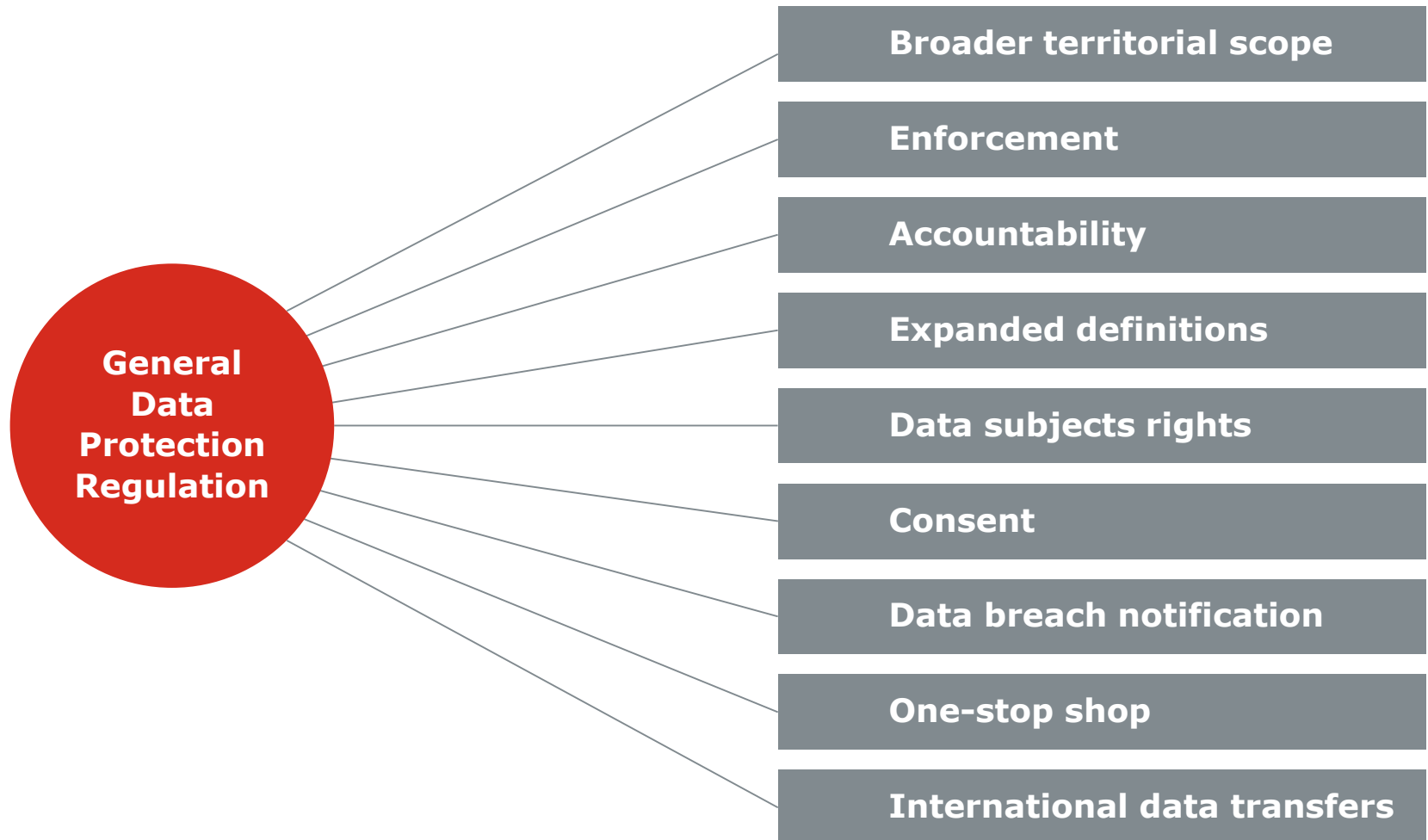
GDPR refresh

Timeline



GDPR refresh

What will change compared to the 1995 EU Data Protection Directive ?



GDPR refresh

Personal data & lifecycle

Any information relating to an identified or identifiable natural person (the 'data subject') [...]

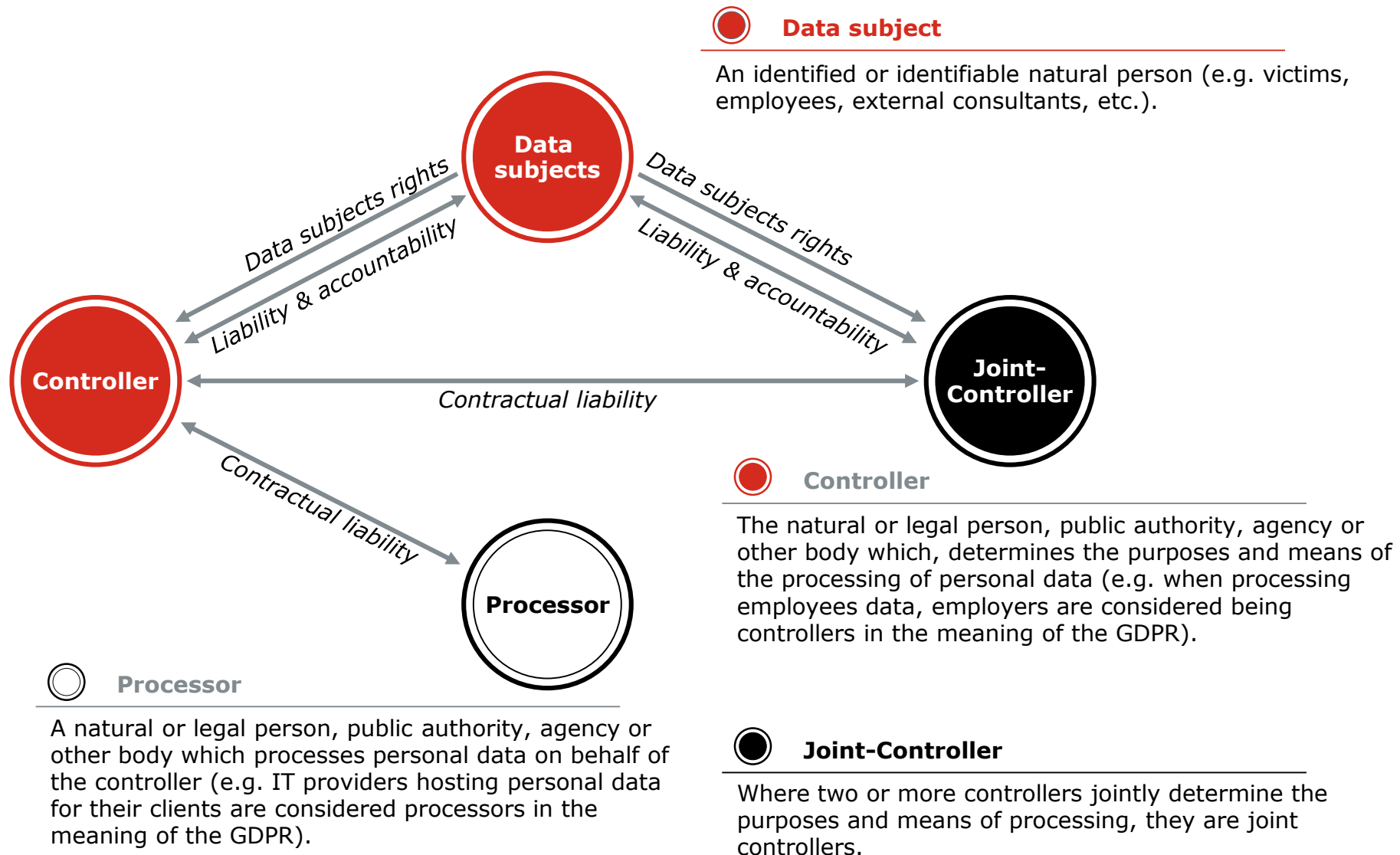
Relating	Identification	Data subject	Reference
<ul style="list-style-type: none">• Content• Purpose• Result	<ul style="list-style-type: none">• Direct• Indirect	<ul style="list-style-type: none">• Not dead• Not unborn• Not legal person	<ul style="list-style-type: none">• Name• ID number• Location data• Online identifier• ...

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction



GDPR refresh

Roles introduced by the GDPR



The upcoming GDPR and the impact on CSIRTs

The upcoming GDPR and the impact on CSIRTs

Recommendations for CSIRTs

-
1. Assess whether CSIRT is controller or processor
 2. Know what is personal data (e.g. IP addresses)
 3. Be aware of legal grounds for processing of personal data
 4. Trust is likely to be enhanced by NIS Directive
 5. Be careful when acting for public or national security
 6. Consult local data protection authority (DPA)
 7. Consider data retention period and draft data retention policy
 8. When exchanging info, assess mandate and mandate of receiving party

The upcoming GDPR and the impact on CSIRTs

1. Assess whether CSIRT is controller or processor

Assessing whether CSIRTs are data controllers or data processors is important. It sets forth **liabilities** and **duties** that CSIRTs have when processing personal data.

Data controller:

- is “*natural or legal person, public authority, agency or any other body which alone or jointly with others, determines **purposes** and **means** of processing of personal data*”
- GDPR Art. 4 (7)

CSIRT is **controller** when it processes data based on **mandate** (not on behalf of another body)

- E.g. CSIRT, during execution of mission, collects IP addresses and communicates them to ISP.

In practice **when CSIRT is controller** it will have to comply with requirements by applicable legislation:

Notification to DPA, when required
(notification is withdrawn by GDPR)

Appointment of a responsible
in charge of data protection issues, etc.

The upcoming GDPR and the impact on CSIRTs

1. Assess whether CSIRT is controller or processor

Data processor:

- is “*natural or legal person, public authority, agency or any other body which processes personal data **on behalf of controller***”.
- GDPR Art. 4 (8)

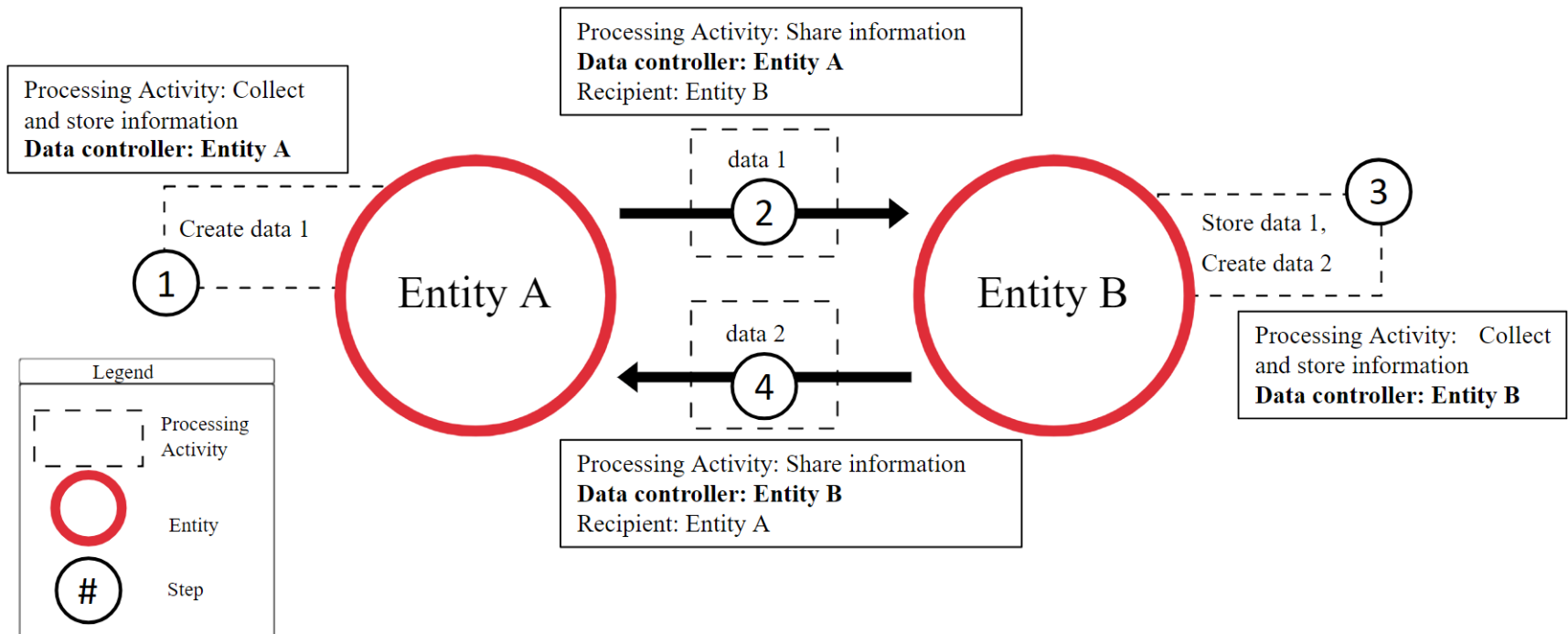
When CSIRT acts **on behalf of law enforcement agency**, other CSIRT, etc., it is **processor** as it does not decide purposes/means.

- E.g. When a CSIRT provides **technical assistance** and processes personal data, whether or not supplied by police,
 - the CSIRT will be data **processor**
 - entity **finally responsible** for the processing is **police** (data **controller**).

The upcoming GDPR and the impact on CSIRTs

1. Assess whether CSIRT is controller or processor

Processing activities and **Data controller** in Information sharing (example model)




The upcoming GDPR and the impact on CSIRTs

2. Know What is personal data (e.g. IP addresses)


IP addresses are personal data (To be on safe side, always consider IP addresses as personal data)




ECJ (Scarlet Extended case): IP addresses processed by ISPs are personal data as they allow users to be precisely identified



WP29, opinion 1/2008: unless controller is position to distinguish with certainty that data correspond to users that cannot be identified, will have to treat all IP info as personal data



ECJ (Patrick Beyer case): dynamic IP addresses, also if only ISP has additional data to identify data subject, are personal data – unless identification is prohibited by law or would require a disproportionate effort

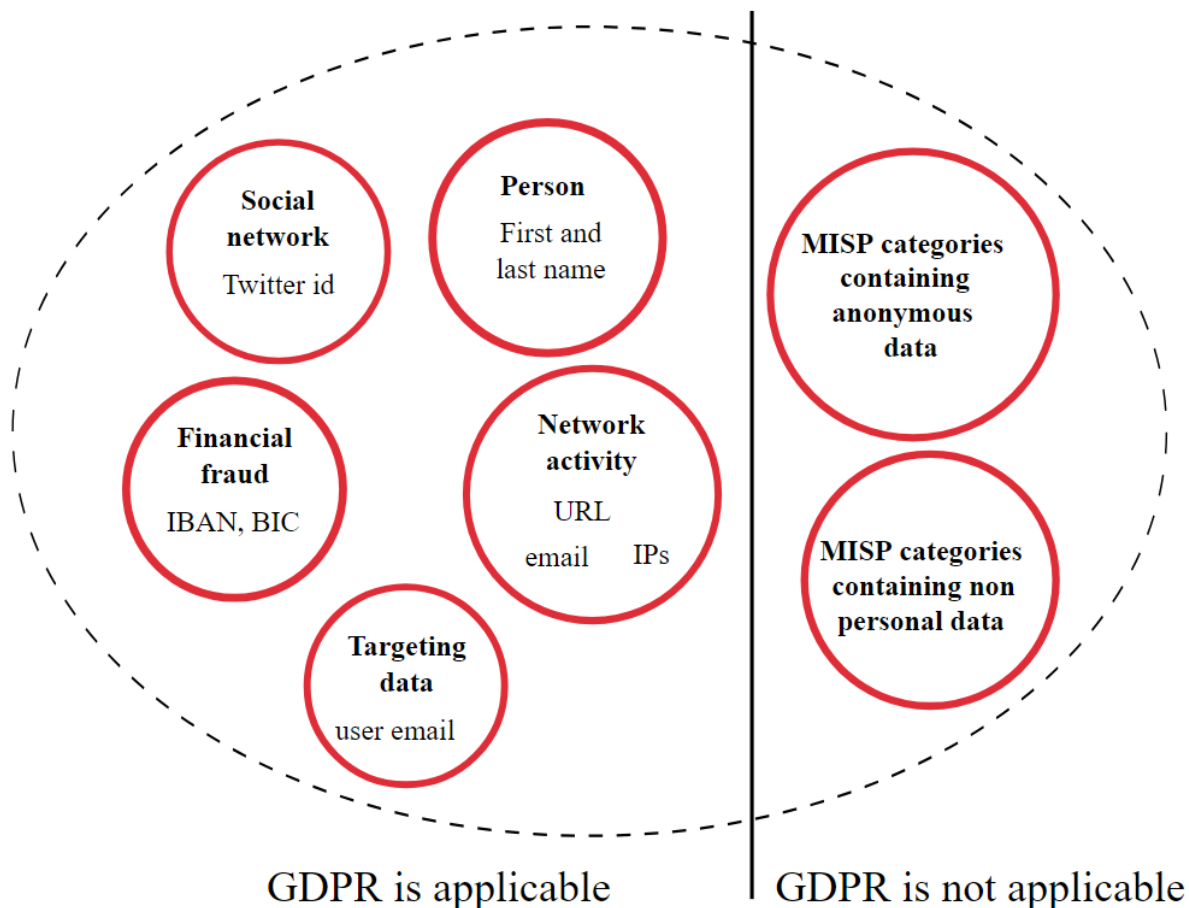


Same applies to user activity data, server logs and traffic data.

The upcoming GDPR and the impact on CSIRTs

2. Know What is personal data (e.g. IP addresses)

Example of MISP attribute categories potentially **involving personal data** (non-exhaustive)



The upcoming GDPR and the impact on CSIRTs

3. Be aware of legal ground for processing of personal data

 Legal grounds that will most likely be used by CSIRTs

It is necessary to determine whether CSIRTs are entitled to process and exchange personal data.

Based on the GDPR, "Processing shall be lawful only if and to the extent that at least one of the following applies:

Consent

The data subject has given consent to the processing of his or her personal data for one or more specific purposes

Contract

Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

Legal

Processing is necessary for compliance with a legal obligation to which the controller is subject;

Vital

Processing is necessary in order to protect the vital interests of the data subject or of another natural person;

Public interest

Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

Legitimate interest

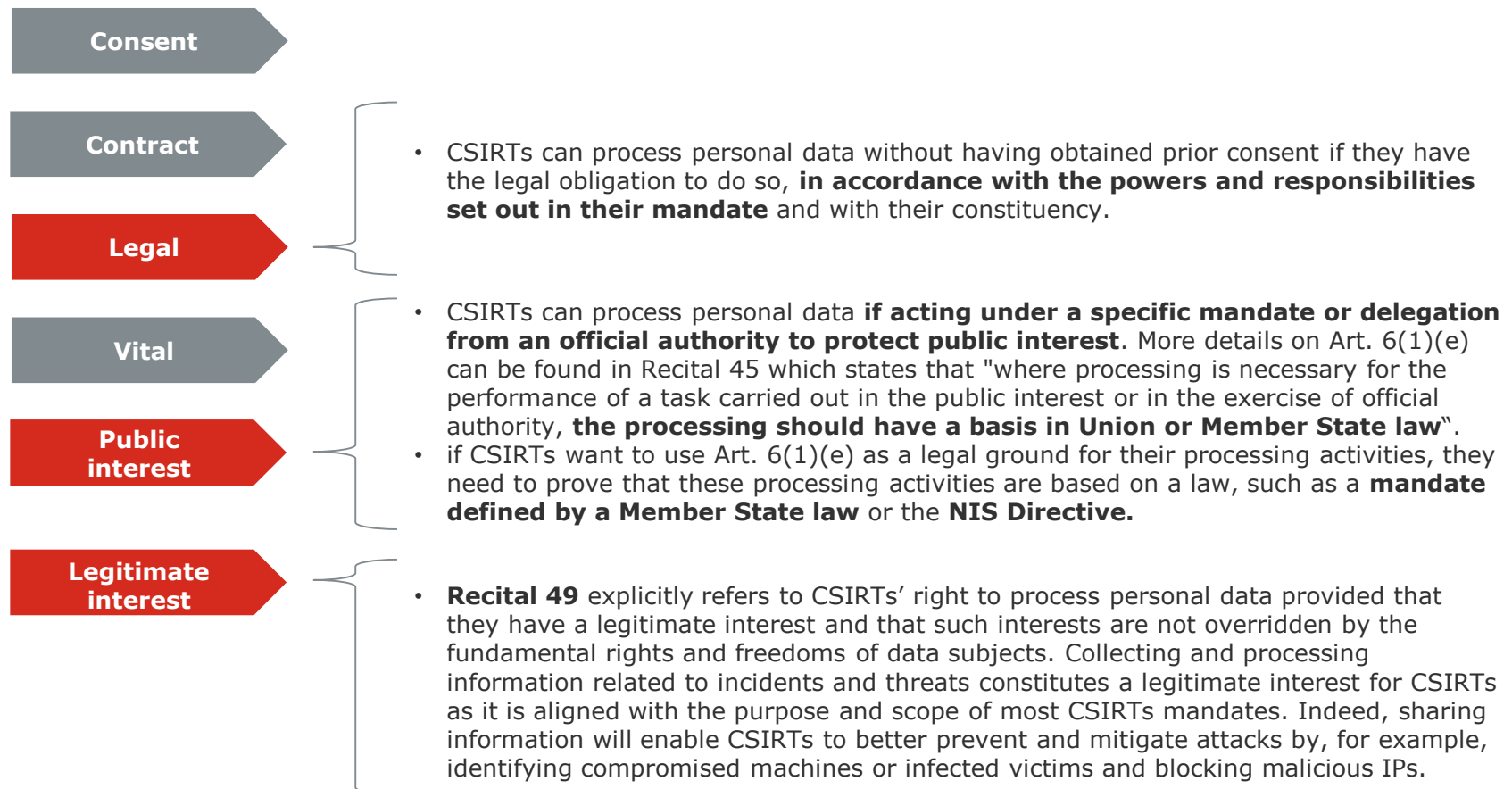
Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

Source : GDPR, Article 6 - Lawfulness of processing

The upcoming GDPR and the impact on CSIRTs

3. Be aware of legal ground for processing of personal data

 Legal grounds that will most likely be used by CSIRTs



The upcoming GDPR and the impact on CSIRTs

4. Trust is likely to be enhanced by NIS Directive

Although for the moment we cannot predict how the Directive will be implemented exactly, it is clear that one of the main purposes of the CSIRTs network is to increase trust between the concerned bodies.

Trust is recognized to be the **most important enabler for cooperation between CSIRTs** by the EU lawmaker.

Dos

- Trust is important, but when sharing info on a bilateral basis, have at least **a simple agreement** in place. An exchange of e-mails between two directors or two employees with delegated powers may be sufficient.

Donts

- Don't ignore the importance and impact of the **NIS Directive**. It will help you to collaborate and share information.

The upcoming GDPR and the impact on CSIRTs

5. Be careful when acting for public or national security

Be careful when acting for public or national security:

- If CSIRTs operate with a specific mandate to fulfil tasks of public safety or national security, they will not be subject to the application of the Data Protection Directive.
- The same applies if CSIRTs operate with a mandate or delegation from a law enforcement agency, judge or prosecutor in framework of a criminal investigation.

It is possible that this will not change significantly under the GDPR. These issues:

- Should be addressed in the policy that we each CSIRT should draft.
- Can be the object of specific consultations with the DPA.

Dos

- Use caution when you process or exchange personal data for public or national security purposes,
- Formalise your mandate from a law enforcement or national security agency in an agreement to clarify what your duties and limits are.

Donts

- Don't disclose personal data that clearly is not useful for the public or national security purposes for which they are required.

The upcoming GDPR and the impact on CSIRTs

6. Consult local data protection authority (DPA)

- DPAs may not be familiar with some issues that CSIRTs face, therefore putting in place communications channels between CSIRTs and DPAs will be beneficial for both parties.
- Ideally the DPA should be consulted before any major activity involving the processing of personal data. In practice, the outcome of the **data protection audit** and the **policy** should be **validated by the DPA**, to ensure legislation is respected and that both the CSIRT and the DPA are on the same page.
- CSIRTs should not be afraid of bringing challenging issues to attention of DPA. This will help both parties to find new solutions.

Dos

- Talk with DPA. Establish **communication channel**, let them know what you do/who you are.
- Ask for **advice** of DPA when not clear whether a data processing activity is legitimate or not
- If you collect and process personal data on a regular basis, retain a **data protection expert** able to provide you with the necessary guidance. The expert can consult with DPA for any issues.

Donts

- Don't assign responsibility to take **decisions** about the processing of personal data to somebody not having the necessary expertise.

The upcoming GDPR and the impact on CSIRTs

7. Consider data retention period and draft data retention policy

- **Data retention clauses** should be included in data protection policy
- Data retention should **not** be unlimited by default, it should be retained for a limited time after an incident has been closed, e.g. six months / one year.
 - This does **not** mean that all info related to an incident or threat should be deleted. However, personal data such as IP addresses, names, e-mail addresses, can be deleted
- The data retention policy can be **discussed with the DPA and/or public prosecutor(s)**
- Info used for **criminal investigations** will be stored **as long as needed** by law enforcement and/or judiciary

Dos

- Ideally keep personal data for a **short period** such as one year
- If you want to store personal data for a longer period, **pseudonymise** and/or **anonymise it**
- Store personal data only for **as long as it** is needed by law enforcement and/or judiciary. During this period **do not use data for any other purpose** not related to investigation.

Donts

- Don't keep personal data forever or for an unreasonably long period.

The upcoming GDPR and the impact on CSIRTs

8. When exchanging info, assess mandate and mandate of receiving party

Not all CSIRTs have same mandate to intervene in any type of incident. Overstepping limits by exchanging info with 3rd party unrelated to its mandate may put at risk value of evidence exchanged.

The receiving CSIRT should first **assess its mandate and the mandate of the requested entity**.

- If any contradiction between these mandates, this can make sharing unjustified /illegal
- The receiving CSIRT should refrain from asking to receive personal data and first carry out an internal legal assessment.
- **Asking the DPA** is recommended.

Dos

- Share personal data that receiving party needs to prevent or respond to a cyber-attack.
- If requested to provide personal data by a foreign law enforcement agency, check with your national authorities if this is legal and allowed.

Don't

- Unless strictly necessary, do not share victims' personal data.

GDPR implementation

Examples for CSIRTs

GDPR Implementation

Examples of gaps & resolution approach for CSIRTs (1/2)

	Policies & procedures	Roles & Responsibilities	Record of Processing Activities	Transparency & Information
Some ways to tackle the gap	<ul style="list-style-type: none"> Review of existing policies & procedures Update or create when needed 	<ul style="list-style-type: none"> Define roles & responsibilities Designate (if applicable) a DPO or coordinator for GDPR 	<ul style="list-style-type: none"> Identify and document your processing activities of personal data Classify those processes in a risk-based approach 	<ul style="list-style-type: none"> Review and update privacy notices and other channels of communication
Starting points		<ul style="list-style-type: none"> Public CSIRTs need a DPO (Art. 37 (1)(a)). The DPO can be shared with other public entities (Art. 37 (3)) Private CSIRTs do not explicitly require a DPO but designation of responsible person 	<ul style="list-style-type: none"> An example of templates for the records specifically for CSIRTs is provided by CIRCL: https://github.com/CIRCL/compliance Risk Methodology (e.g. based on WP29 and/or ENISA Guidelines*) 	<ul style="list-style-type: none"> Privacy Notice templates. Examples of such templates can be found on other CSIRT websites, e.g. CIRCL's privacy notice under creative commons https://www.circl.lu/privacy CSIRT can do a privacy notice for services with specific data retention requirements e.g. PGP servers

* ENISA, "Guidelines for SMEs on the security of personal data processing", December 2016

ENISA, "Recommendations for a methodology of the assessment of severity of personal data breaches", December 2013

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

GDPR Implementation

Examples of gaps & resolution approach for CSIRTs (1/2)

	Training & Awareness	Data Subject Rights	Data Breach Incident Management	International Data Transfers
Some ways to tackle the gap	<ul style="list-style-type: none">Organize dedicated training sessions / implement an awareness programRegularly communicate	<ul style="list-style-type: none">Define, document and implement the processes to manage data subject rights	<ul style="list-style-type: none">Define / update and implement incident management procedures, covering the personal data aspects	<ul style="list-style-type: none">Identify these transfers based on the processing activitiesEstablish the expected level of complianceImplement required safeguards
Starting points	<ul style="list-style-type: none">Tailored awareness sessions & trainingsFor CSIRTs in the CSIRT network, training materials are available through the different Connecting Europe Facility projects	<ul style="list-style-type: none">Procedure to handle data subject rightsMany CSIRTs already have the tools and expertise to handle constituency requests. For example, CSIRTs can create custom email templates in their incident management tool (e.g. RTIR*)	<ul style="list-style-type: none">Many CSIRTs already have a formal incident management process. In those cases, an update to those processes is sufficient.	<ul style="list-style-type: none">CSIRTs are usually sharing information outside the EU, usually for public interest. International data transfers should be documented.

* RTIR: Request Tracker for Incident Response

Conclusion

Conclusion

Nothing in the EU legislation prevents **CSIRTs** from **processing** personal data

It is clear from the GDPR that **CSIRTs can and should exchange information to fulfil their mission**, including personal data

CSIRTs can process personal data to extent strictly necessary and proportionate to **ensure network and information security** – it is a legitimate interest of the data controller (recital 49 of GDPR)

Data retention is also important, based on the principle of proportionality and taking into account the data subject's rights

CSIRTs should work in **close cooperation with the DPAs**

Q&A