

INTRODUCTION

A number of EU laws require some form of reporting in the event of a data breach or other cybersecurity incident. Such notification requirements differ depending on many variables, such as the entity in question and the type of incident at hand. Hence, many organizations are faced with the challenge of navigating a complex legal environment to identify whether a certain law applies in their case, what reporting obligations it entails, and whether, and how, they may overlap with obligations under other EU digital legislation.

This chart is meant as a guide to provide an overview of digital incident notification and information sharing requirements across several EU digital laws, namely the General Data Protection Regulation, the Law Enforcement Directive, the e-Privacy Directive, the Data Governance Act, the Data Act, the Network and Information Security Directive 2, the Digital Operational Resilience Act, the Payment Services Directive 2, the Cyber Resilience Act and the Artificial Intelligence Act. The first iteration of this chart does not capture all EU laws with similar requirements; rather, it focuses on laws that either have broad material scope or have sectoral significance.



Laws included in the chart apply to a range of events i.a. personal data breaches, cybersecurity incidents, threats and vulnerabilities, and serious AI system incidents. Under a given law, the chart names

the entity subject to the incident notification requirements. It lists the types of incidents covered in that legislation and links them to the reporting entity. It identifies the entity that should be the recipient of the notification, be it a user, a national competent authority, or another body. It clarifies whether the reporting is mandatory or voluntary and the notification timeline. Finally, the chart identifies what triggers the notification in the first place.

Some of the laws covered in this resource also require or recommend that the entity receiving the notification communicate certain information related to the notification to other entities. Such requirements are covered in the “further and related information sharing” sections.

With respect to the Digital Operational Resilience Act, the chart also includes the notification timelines in the draft Regulatory Technical Standard which is subject to change. Practitioners are invited to consult the text of the relevant legislation, secondary legislation, and guidelines or other instruments as provided by the European institutions, courts, competent authorities or other bodies for further clarification, as well as industry best practices and sectoral law requirements where relevant.

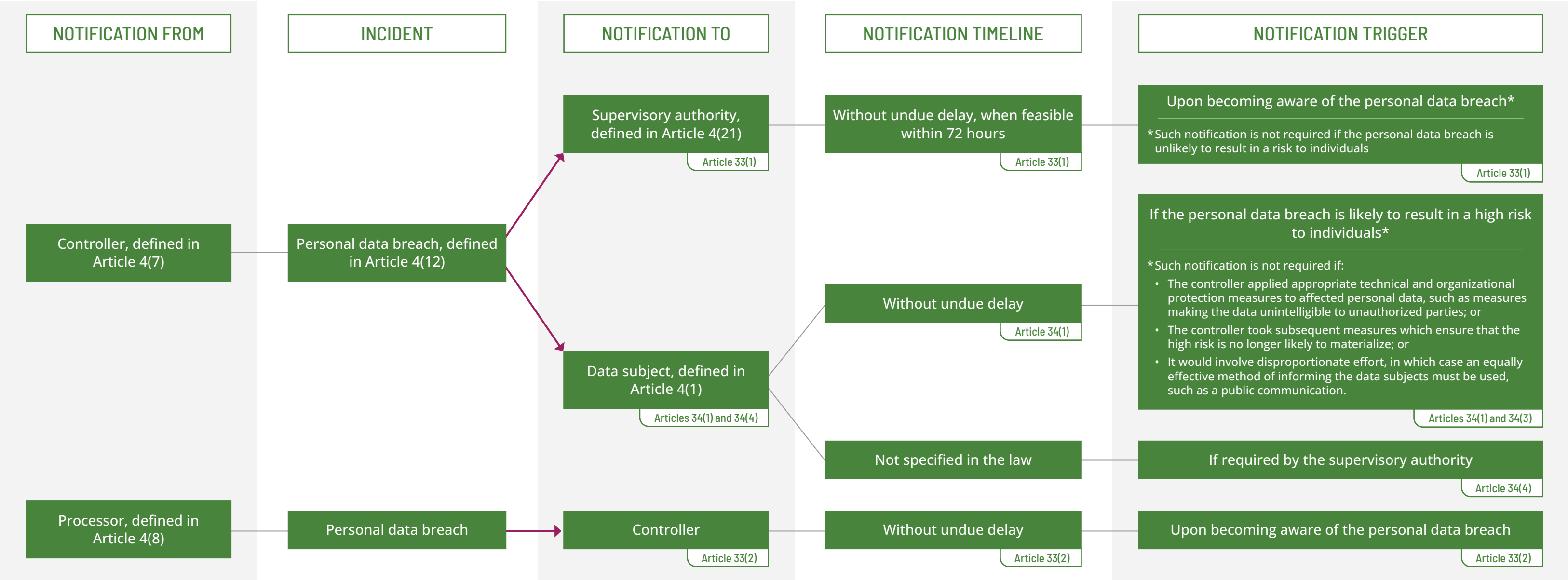
KEY:

-  Obligatory notification/communication
-  Voluntary notification/communication

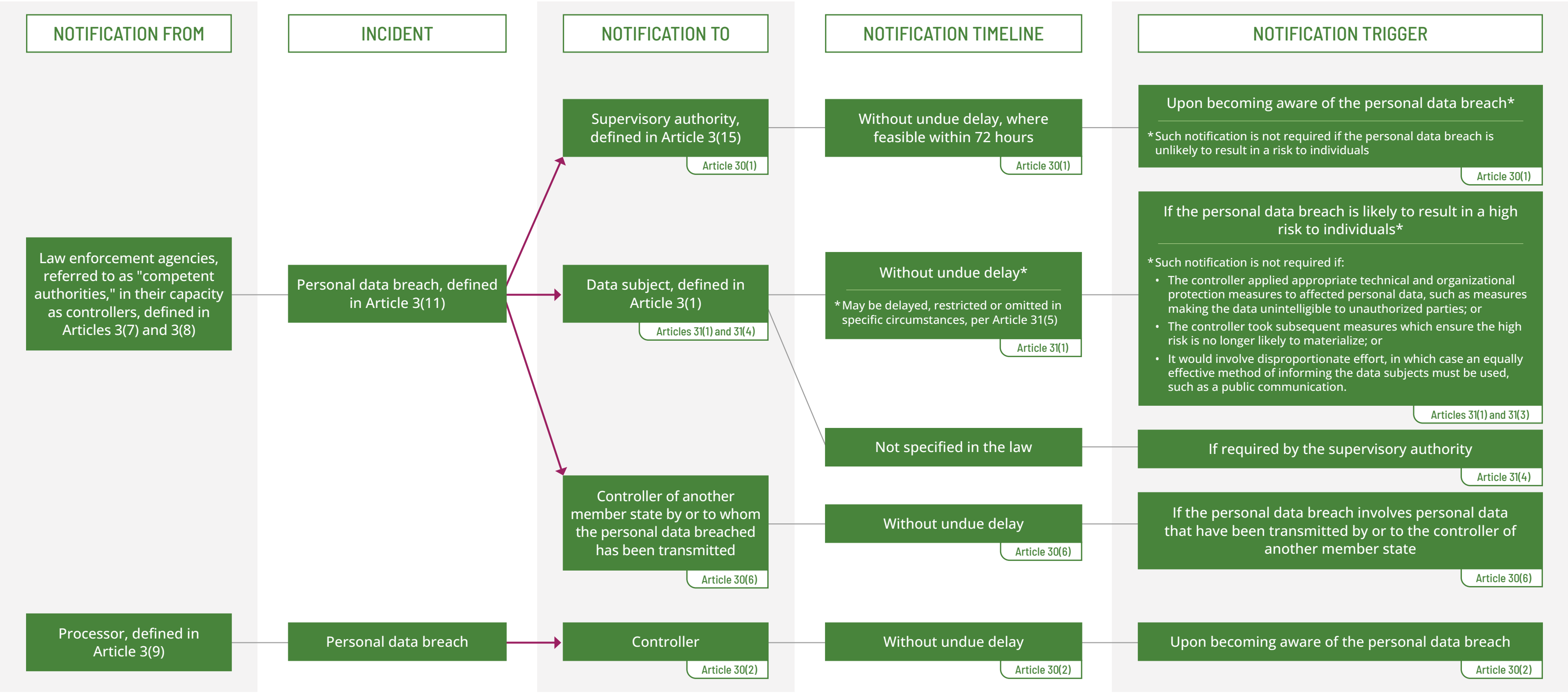
ADDITIONAL RESOURCES:

[European Strategy for Data – Overview of New Regulations](#)

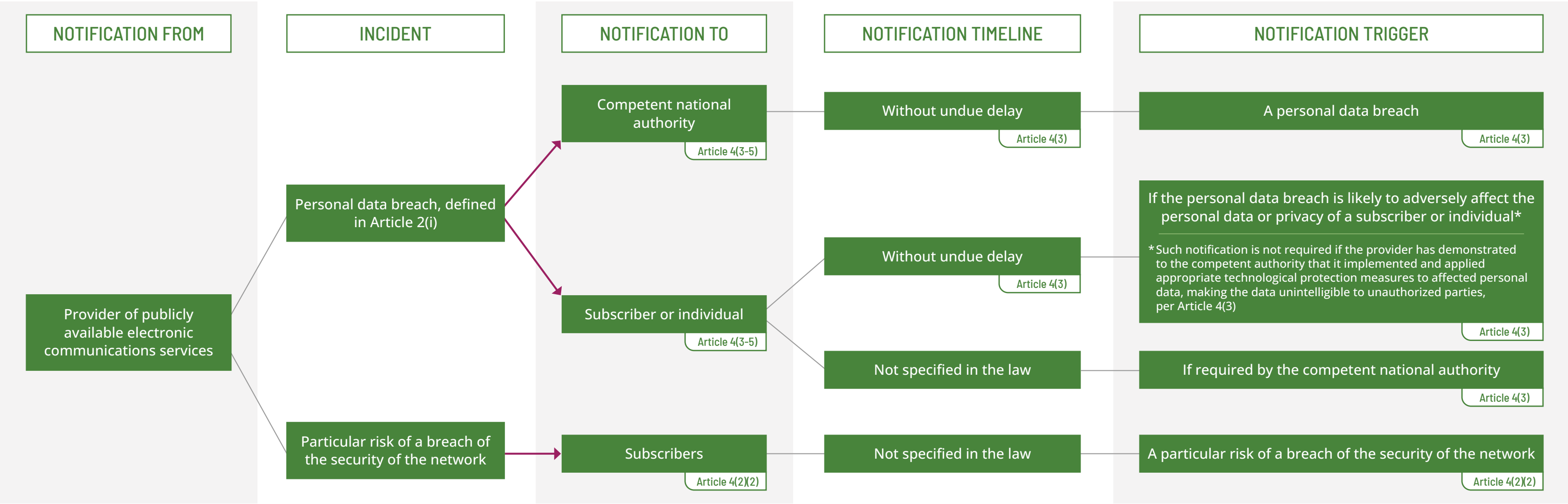
GENERAL DATA PROTECTION REGULATION – 2016/679



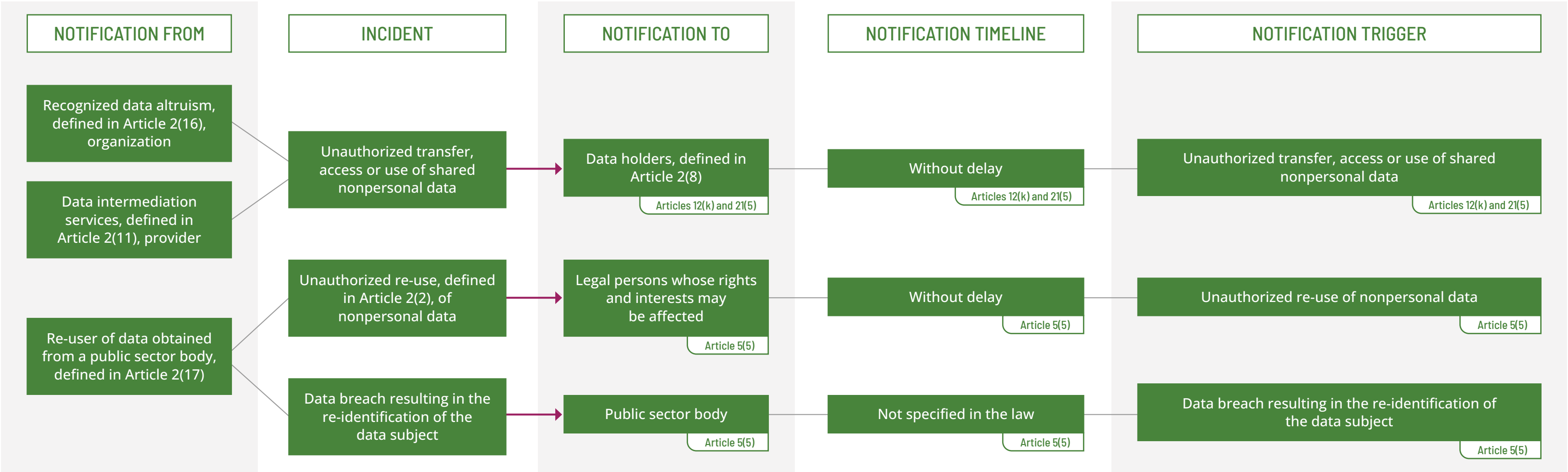
LAW ENFORCEMENT DIRECTIVE – 2016/680



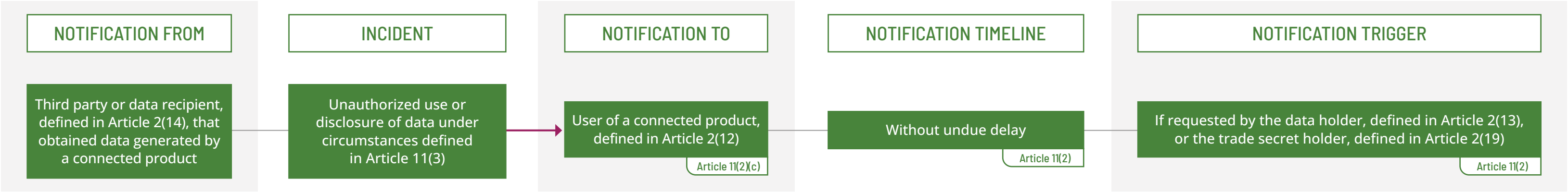
E-PRIVACY DIRECTIVE – 2002/58/EC



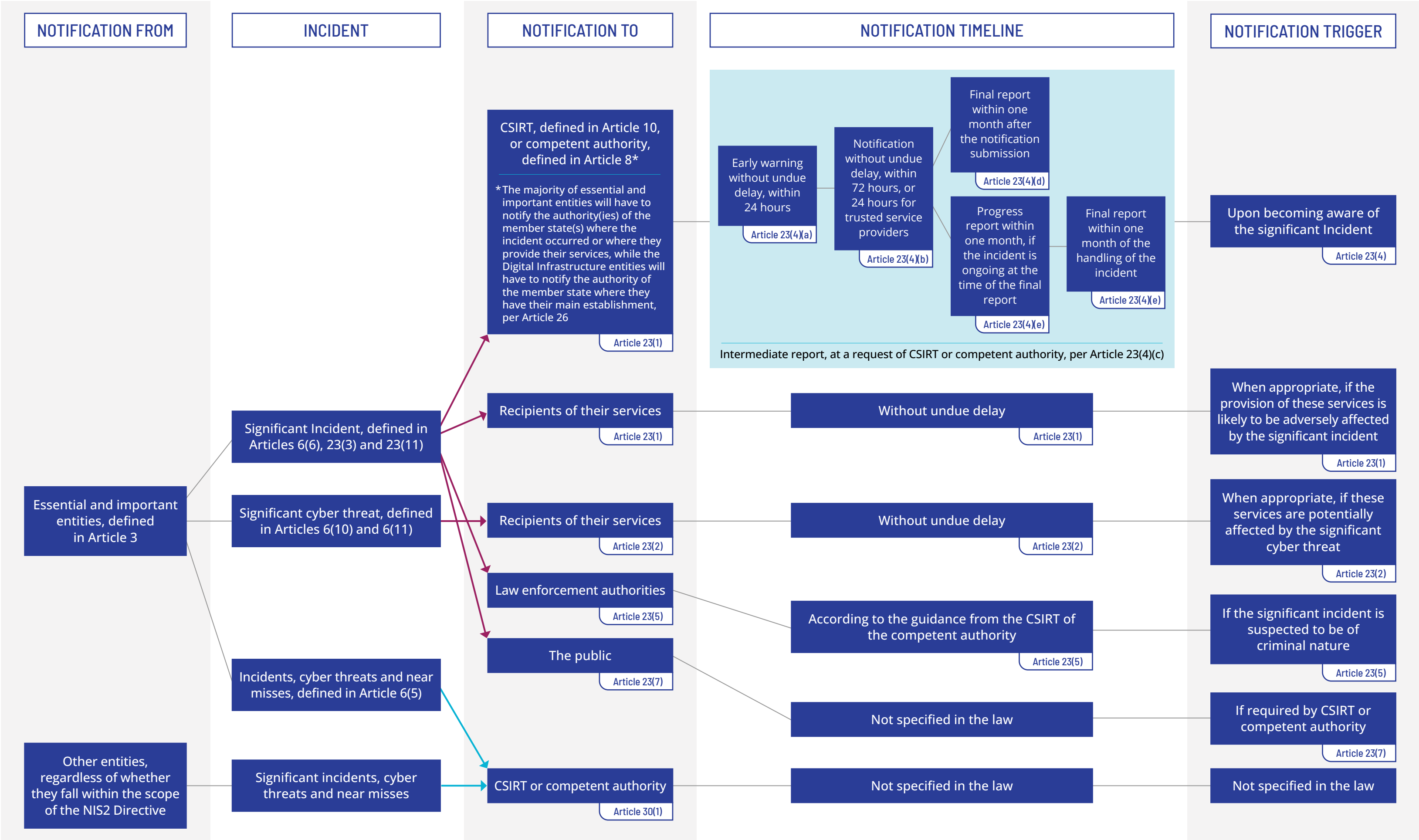
DATA GOVERNANCE ACT – 2022/868



DATA ACT – 2023/2854



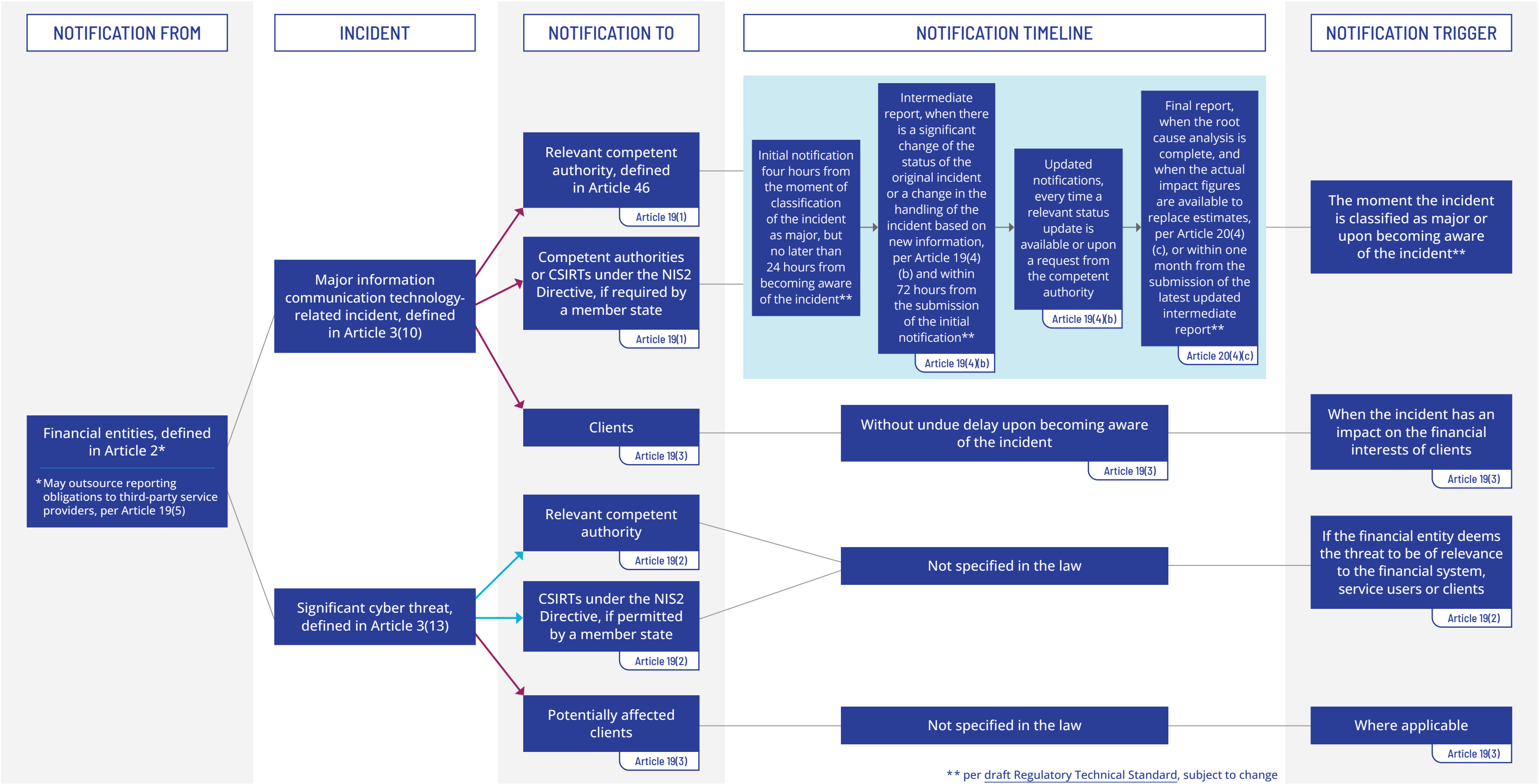
NETWORK AND INFORMATION SECURITY DIRECTIVE 2 – 2022/2555



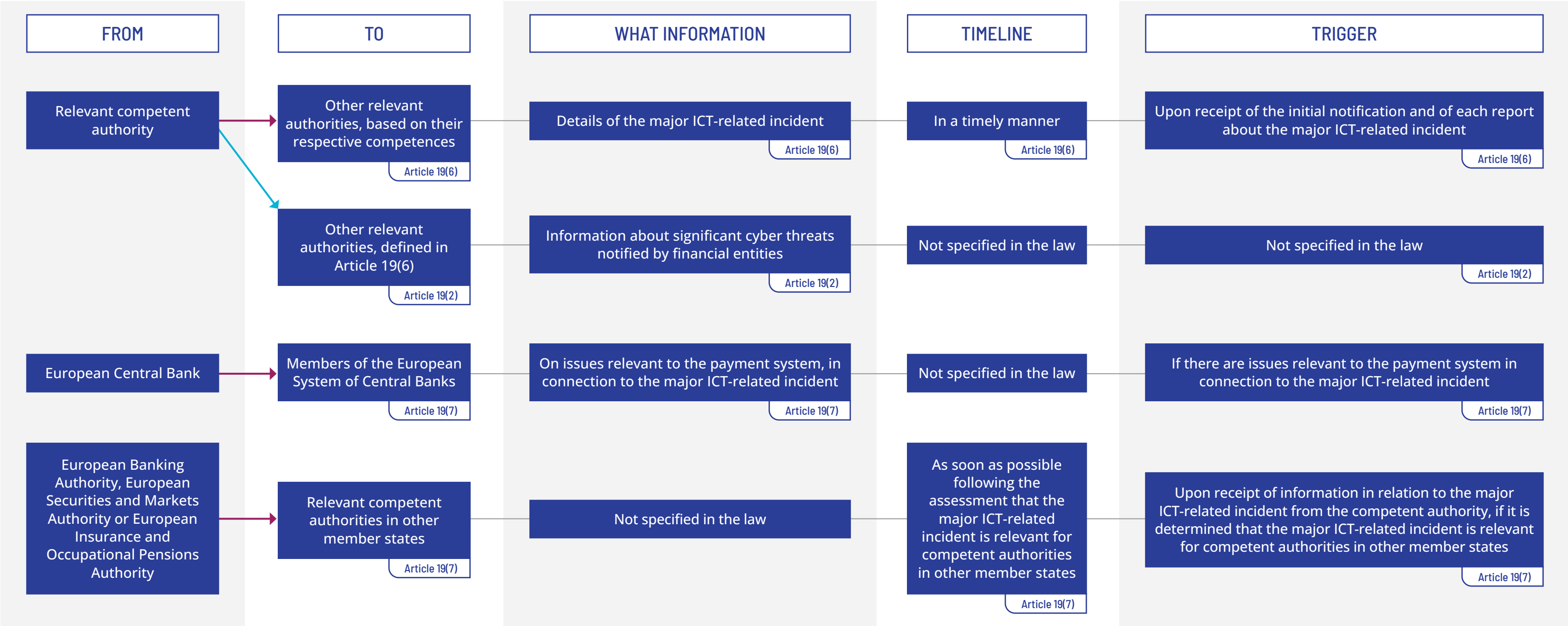
NETWORK AND INFORMATION SECURITY DIRECTIVE 2 – 2022/2555 | FURTHER AND RELATED INFORMATION SHARING

FROM	TO	WHAT INFORMATION	TIMELINE	TRIGGER
Entities that fall within the scope of the NIS2 Directive and other relevant entities	Entities that fall within the scope of the NIS2 Directive and other relevant entities <small>Article 29(1)</small>	Relevant cybersecurity information, e.g. information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise and adversarial tactics <small>Article 29(1)</small>	Not specified in the law	When such information sharing aims to prevent, detect, respond to or recover from incidents or to mitigate their impacts or enhances the level of cybersecurity <small>Article 29(1)</small>
Notified competent authority	CSIRT <small>Article 23(1)</small>	The notification of a significant incident received from an essential or important entity <small>Article 23(1)</small>	Upon receipt of the notification <small>Article 23(1)</small>	When an essential or important entity notifies the competent authority of a significant incident <small>Article 23(1)</small>
	Competent authorities under the Critical Entities Resilience Directive <small>Article 23(10)</small>	Information about notified significant incidents, incidents, cyber threats and near misses <small>Article 23(10)</small>	Not specified in the law	When significant incidents, incidents, cyber threats and near misses are notified by entities identified as critical entities under the Critical Entities Resilience Directive <small>Article 23(10)</small>
	Single point of contact <small>Articles 23(1) and 30(2)</small>	Relevant information notified by essential and important entities <small>Article 23(1)</small>	In due time <small>Article 23(1)</small>	In case of a cross-border or cross-sectoral significant incident <small>Article 23(1)</small>
		Information about voluntary notifications of incidents, significant incidents, cyber threats and near misses <small>Article 30(2)</small>	Not specified in the law	When necessary <small>Article 30(2)</small>
Notified CSIRT or competent authority	Other affected member states and ENISA <small>Article 23(6)</small>	Information on the notified significant incident <small>Article 23(6)</small>	Without undue delay <small>Article 23(6)</small>	When a significant incident concerns two or more member states and when otherwise appropriate <small>Article 23(6)</small>
Single point of contact, defined in Article 8(3)	Single points of contact of other affected member states <small>Article 23(8)</small>	Notifications received <small>Article 23(8)</small>	Not specified in the law	When it is requested by CSIRT or the competent authority <small>Article 23(8)</small>
CSIRT and competent authorities of other member states concerned	The public <small>Article 23(7)</small>	About the significant incident <small>Article 23(7)</small>	After consulting the entity concerned <small>Article 23(7)</small>	When public awareness is necessary to prevent a significant incident or to deal with an ongoing significant incident, or when its disclosure is otherwise in the public interest <small>Article 23(7)</small>
	ENISA <small>Article 23(9)</small>	A summary report, including anonymized and aggregated data on significant incidents, incidents, cyber threats and near misses notified, including voluntarily	Every three months <small>Article 23(9)</small>	
Competent authority	Data protection authority of own member state <small>Article 35(1)</small>	That an infringement by an essential or important entity of their obligations under the NIS2 Directive can entail a personal data breach as defined in the GDPR <small>Article 35(1)</small>	Without undue delay <small>Article 35(1)</small>	When an infringement by an essential or important entity of their obligations under the NIS2 Directive can entail a personal data breach as defined in the GDPR <small>Article 35(1)</small>
European Union Agency for Cybersecurity	CSIRTs network and the Cooperation Group, defined in Article 14 <small>Article 23(9)</small>	Its findings on notifications received <small>Article 23(9)</small>	Every six months <small>Article 23(9)</small>	N/A

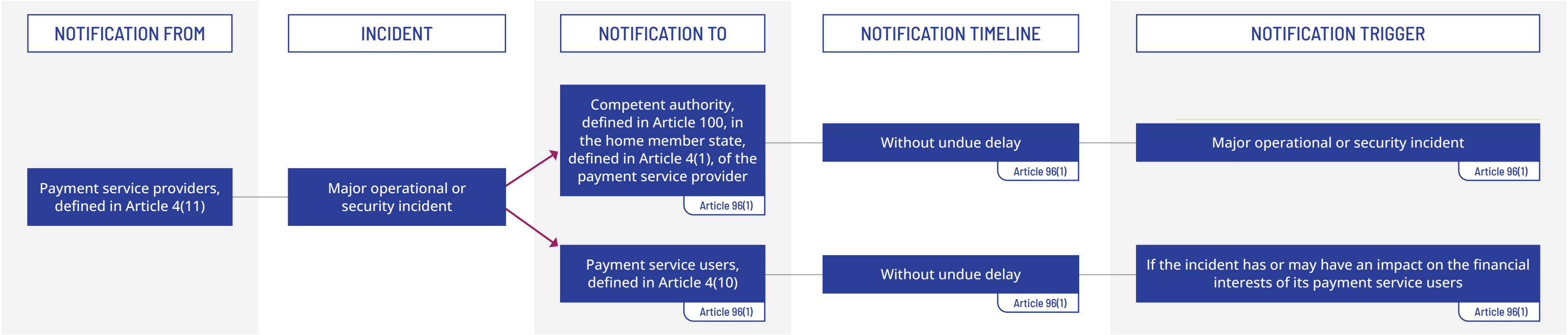
DIGITAL OPERATIONAL RESILIENCE ACT – 2022/2554



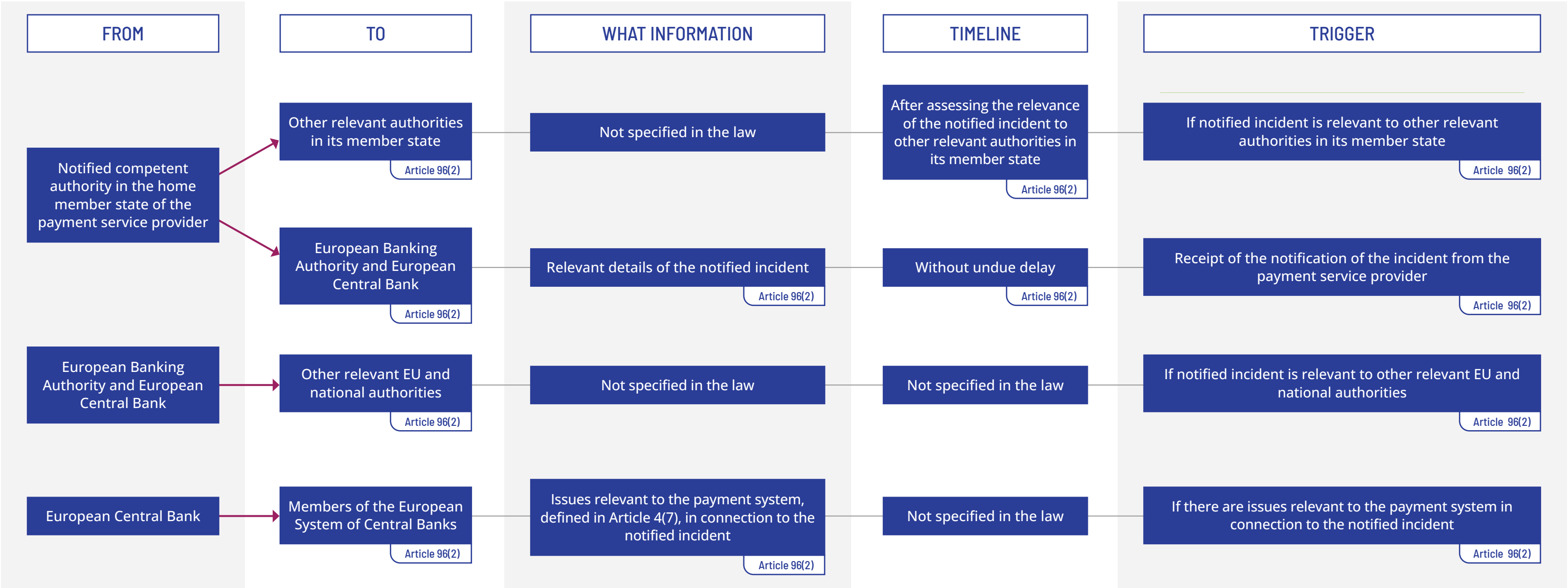
DIGITAL OPERATIONAL RESILIENCE ACT – 2022/2554 | FURTHER AND RELATED INFORMATION SHARING



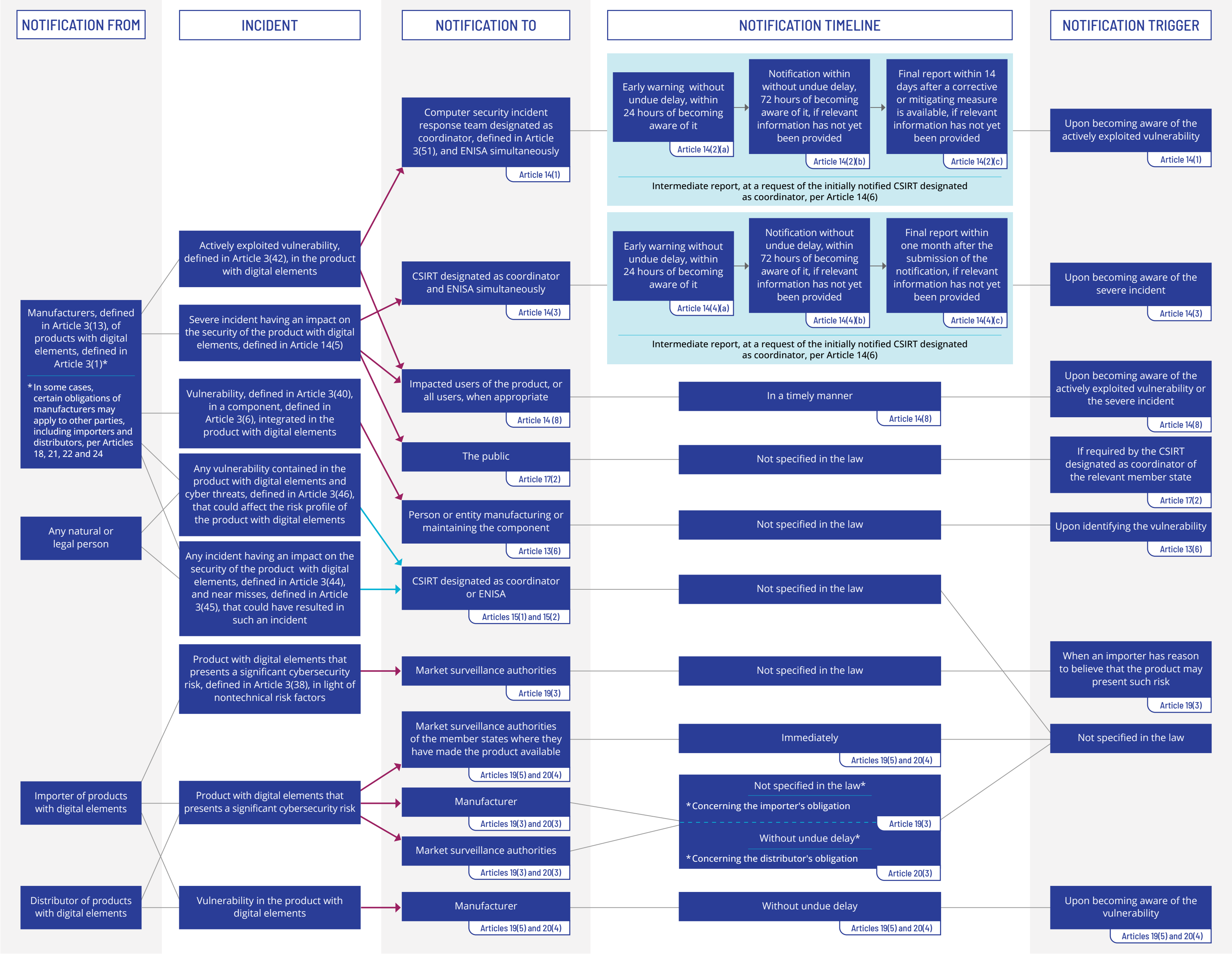
PAYMENT SERVICES DIRECTIVE 2 – 2015/2366



PAYMENT SERVICES DIRECTIVE 2 – 2015/2366 | FURTHER AND RELATED INFORMATION SHARING



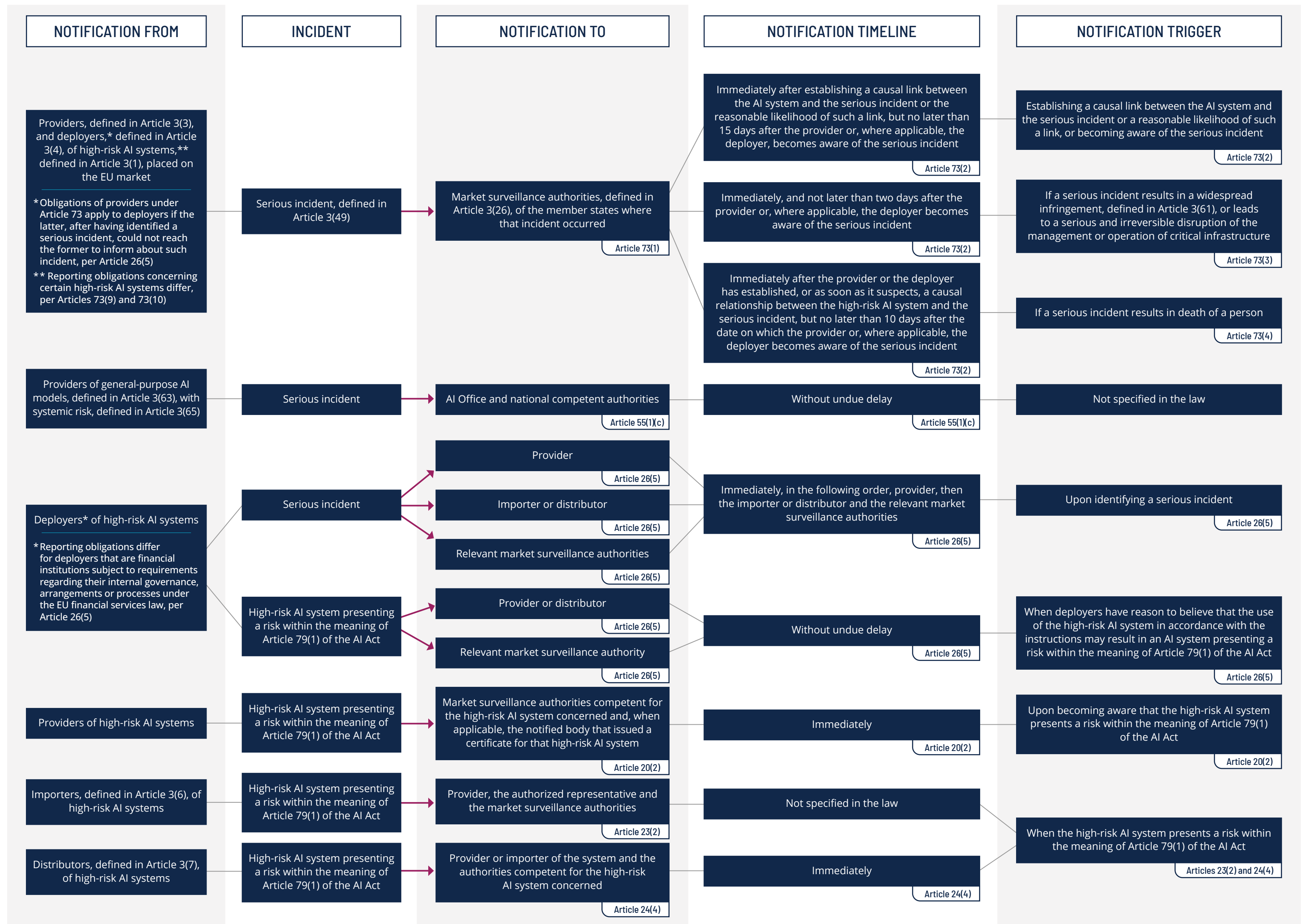
CYBER RESILIENCE ACT – 2024/2847



CYBER RESILIENCE ACT – 2024/2847 | FURTHER AND RELATED INFORMATION SHARING

FROM	TO	WHAT INFORMATION	TIMELINE	TRIGGER
Notified CSIRT designated as coordinator	Impacted users of the product with digital elements, or all users when appropriate	Of the notified actively exploited vulnerability or severe incident having an impact on the security of the product, when necessary, also risk mitigation and corrective measures that users can deploy	Not specified in the law	If the manufacturer fails to inform the users about the actively exploited vulnerability or severe incident having an impact on the security of the product in a timely manner and the CSIRT considers it proportional and necessary to inform them for preventive or mitigative purposes
	Manufacturer of the product with digital elements	Of an actively exploited vulnerability or a severe incident having an impact on the security of a product	Without undue delay	If a natural or legal person other than the manufacturer notifies an actively exploited vulnerability or a severe incident having an impact on the security of a product
	Market surveillance authorities of its respective member state	Notified information necessary for the market surveillance authorities to fulfill their obligations under the CRA	Not specified in the law	After receiving a notification of an actively exploited vulnerability or a severe incident having an impact on the security of a product
	CSIRTs designated as coordinators on the territory where the product has been made available, according to the manufacturer	The notification received	Without delay* * May be delayed in exceptional circumstances	After receiving the notification
	The public	About a severe incident having an impact on the security of the product	After consulting the manufacturer concerned	When public awareness is necessary to prevent or mitigate a severe incident having an impact on the security of the product or to handle an ongoing incident, or when disclosure is otherwise in the public interest
ENISA	European cyber crisis liaison organisation network	Notified information	Not specified in the law	If notified information is relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level

ARTIFICIAL INTELLIGENCE ACT - 2024/1689



ARTIFICIAL INTELLIGENCE ACT – 2024/1689

FURTHER AND RELATED INFORMATION SHARING

