Council of the European Union

Brussels, 25 February 2025
(OR. en)

6527/25
ADD 1

Interinstitutional File:
2025/0036(NLE)

CYBER 52
IPCR 11
RELEX 241
JAI 235
JAIEX 17
POLMIL 42
HYBRID 19
TELECOM 62
COSI 37

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	24 February 2025
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2025) 66 final
Subject:	ANNEXES to the Proposal for a COUNCIL RECOMMENDATION for an EU Blueprint on cybersecurity crisis management

Delegations will find attached document COM(2025) 66 final.

Encl.: COM(2025) 66 final

EUROPEAN
COMMISSION

Brussels, 24.2.2025
COM(2025) 66 final

ANNEXES 1 to 3

ANNEXES

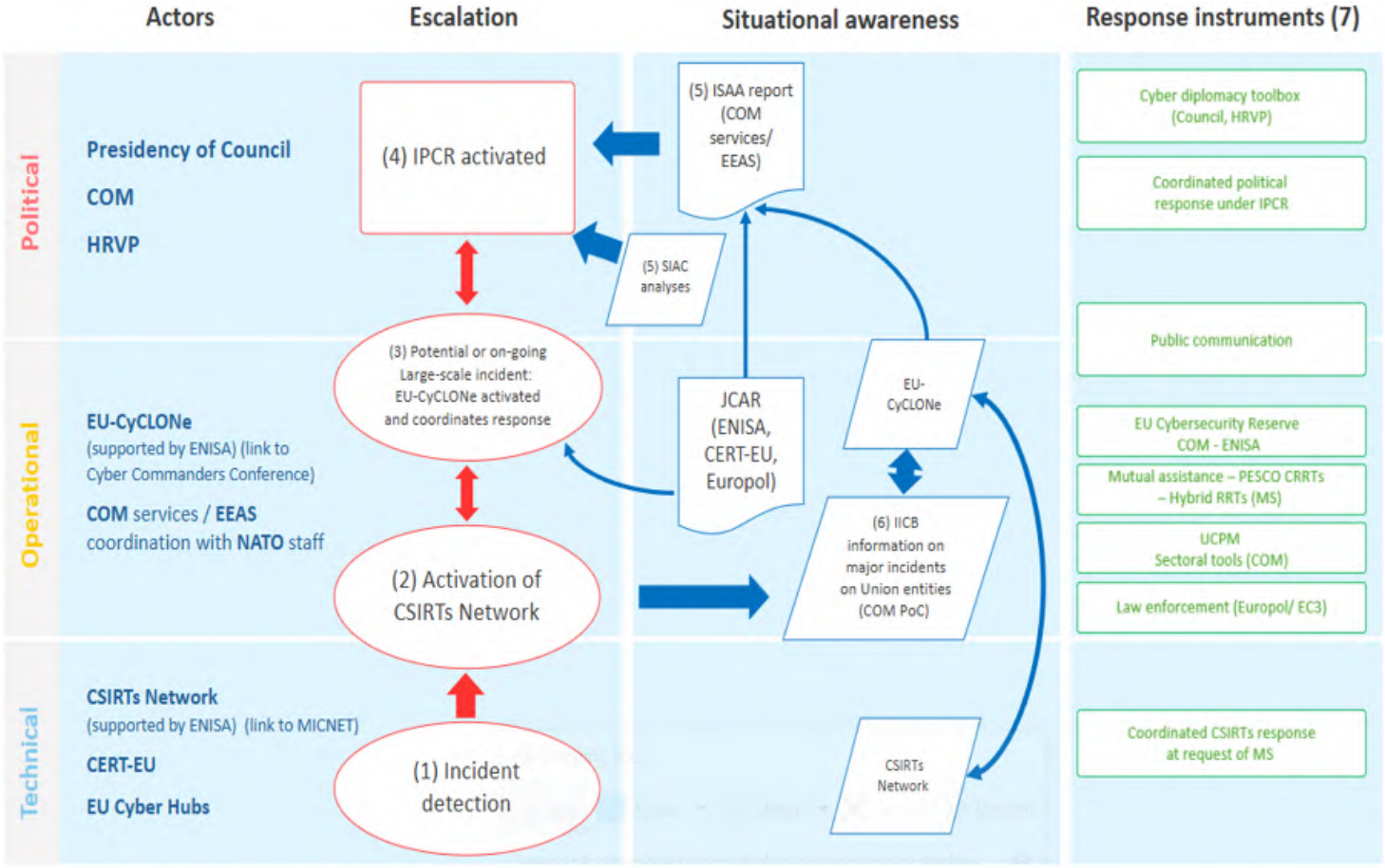
to the

Proposal for a COUNCIL RECOMMENDATION

for an EU Blueprint on cybersecurity crisis management

ANNEX I – The Union Blueprint for responding to a cybersecurity crisis

The diagram below illustrates and summarises the Union Cyber Blueprint: who talks to whom in a Union cybersecurity crisis, in accordance with relevant EU-crisis mechanisms in Annex II below. Such a crisis will inevitably involve a real-world impact in one or more critical sectors, requiring close coordination between the cyber community and sectoral and civil protection response mechanisms. A cyber incident may be part of wider hybrid campaigns and the cyber response therefore should be coordinated with other actions in line with the Union's preparedness strategy.



(1) CSIRTs and/or Cross-border Cyber Hubs detect a large- scale cybersecurity incident.
(2) CSIRTs Network escalates in accordance with internal procedures.
(3) EU-CyCLONe coordinates operational response in the case of a large-scale incident.
(4) Council Presidency, in consultation with Member States, the Commission and the High Representative, determines whether to activate or deactivate the EU (IPCR) crisis arrangements.
(5) Where the IPCR is activated, ISAA reports developed by the Commission services and EEAS inform discussions. EU-CyCLONe and JCAR should provide input to ISAA. Council is also informed by SIAC analyses.
(6) CERT- EU is responsible for the operational response to crises affecting Union entities; relevant information may be provided to EU-CyCLONe by the IICB via the Commission as point of contact.
(7) Council, EU-CyCLONe and CSIRTs Network have overview of responses at political, operational and technical levels, respectively.

ANNEX II- RELEVANT UNION-LEVEL ACTORS (ENTITIES AND NETWORKS) AND CRISIS MANAGEMENT MECHANISMS

(1) Relevant Union-level actors across the cyber crisis management life cycle

Level/ Stage	Preparedness	Detection	Response	Recovery
Political	• Council • Commission • EEAS		• Council • Commission • EEAS	
Operational	• EU-CyCLONe • ENISA • Commission • Europol		• EU-CyCLONe • Commission • ENISA • CERT-EU (for incidents affecting Union entities) • Europol	• ENISA
Technical	• CSIRTs Network • Cross-Border Cyber Hubs • CERT-EU	• CSIRTs Network • Cross-Border Cyber Hubs • CERT-EU	• CSIRTs Network • CERT-EU	• CSIRTs Network • CERT-EU

(2) Roles and competences of the relevant Union-level actors (in alphabetical order) in relation to cyber crisis management

Actor	Level	Role and competence	Reference
CERT-EU	Technical / Operational	Coordinates the response and the management of major incidents affecting Union entities. Member of the CSIRTs Network. Supports the Commission in EU-CyCLONe. Acts as the cybersecurity information exchange and incident response coordination hub, facilitating the exchange of	Regulation (EU, Euratom) 2023/2841

Actor	Level	Role and competence	Reference
		information regarding incidents, cyber threats, vulnerabilities and near misses among Union entities and counterparts. Requests the deployment of the EU Cybersecurity Reserve on behalf of Union entities. Cooperates with the NATO Cybersecurity Centre on the basis of their Technical Agreement.	
Presidency of the Council of the EU	Political	Decides (except where the solidarity clause is activated under TFEU Article 222 of the Treaty on the Functioning of the European Union) whether to activate or deactivate the IPCR, at the invitation of a Member State, in consultation affected Member States as appropriate, as well as the Commission and the HR, and when to escalate or deescalate from one mode of activation to the other.	Article 16 of the Treaty on European Union Council Implementing Decision (EU) 2018/1993
Cross-border cyber hubs	Technical	Formed of three or more national cyber hubs, they ensure exchange of relevant information related to cyber threats, near misses, indicators of compromise, cyber alerts within the cross-border hub. Cooperate closely with the CSIRTs Network to share information. Provide information relating to a potential or ongoing large-scale cybersecurity incident to Member States' authorities and the Commission through EU-CyCLONe and the CSIRTs Network.	Regulation (EU) 2025/38
CSIRTs Network	Technical	Exchanges relevant information about incidents, near misses, cyber threats, risks, and vulnerabilities. At the request of a member potentially affected by an incident, the Network exchanges and discusses information in relation to that incident and associated cyber	Article 15 of Directive (EU) 2022/2555

Actor	Level	Role and competence	Reference
		threats. The Network can also implement a coordinated response to an incident that has been identified within the jurisdiction of a requesting member. Receives information from Member States regarding their requests to the EU Cybersecurity Reserve.	
Cyber Commanders conference		A forum for cyber commanders at the national level within Member States to collaborate and exchange vital information regarding ongoing cyberspace operations and strategies for mitigating large-scale cyber incidents. It is organised by the rotating presidency of the Council of the European Union with the support of European Defence Agency (EDA), European External Action Service (EEAS), and the EU Military Staff (EUMS).	Cyber Defence Joint Communication
Commission	Operational / Political	Ensuring the smooth functioning of the Internal market Providing analytical reports (ISAA) for the IPCR mechanism General preparedness actions, including managing the Emergency Response Coordination Centre and the Common Emergency Communications and Information system. Observer in EU-CyCLONe and Member in case of potential or ongoing large-scale incident. Observer in the CSIRTS Network. Overall responsibility for the implementation of the EU Cybersecurity Reserve. Point of contact of the Inter-institutional Cybersecurity Board for sharing relevant information in relation to major incidents with EU-CyCLONe.	Article 17 of the Treaty on European Union Implementing Decision (EU) 2018/1993 Decision No 1313/2013/EU of the European Parliament and of the Council Directive (EU) 2022/2555 Regulation (EU) 2025/38Regulation (EU, Euratom) 2023/2841

Actor	Level	Role and competence	Reference
		Strategic oversight of the Galileo Security Monitoring Centre. (GSMC) Consulted by Presidency of the Council on decisions to activate or deactivate the IPCR. Commission services develop, with the EEAS, the ISAA report.	
European Cybersecurity Agency (ENISA)	Technical / operational	Provides the secretariat for the CSIRTs Network and EU-CyCLONe. Helps develop a common response to large-scale cross border incidents or crises by: Aggregating and analysing reports from national sources Ensuring flow of information between technical, operational and political levels Facilitating handling of incidents Supporting Union entities with regards to public communication. Testing incident response capabilities. Operates and administrates the EU Cybersecurity Reserve, partly or fully, as provided in the Cyber Solidarity Act. Reviews and assesses threats, known vulnerabilities and mitigation actions for a specific significant or large-scale cyber incident. Prepares an incident review report	NIS 2 Directive (EU) 2022/2555 Regulation (EU) 2019/881 Regulation (EU) 2025/38 Regulation (EU) 2024/2847
European cyber crisis liaison organisation network (EU-CyCLONe)	Operational	Supports the coordinated management of large-scale cybersecurity incidents and crises at operational level Ensures the regular exchange of relevant information among Member States and Union institutions, bodies, offices, and agencies. Coordinates the management of	Directive (EU) 2022/2555 Regulation (EU) 2025/38

Actor	Level	Role and competence	Reference
		large-scale cybersecurity incidents and crises and supports decision-making at political level in relations to such incidents and crises. Assesses the consequences and impact of relevant large-scale cybersecurity incidents and crises and proposes possible mitigation measures. Develops, together with ENISA, the template to facilitate submission of requests for support from the EU Cybersecurity Reserve. Receives information from Member States regarding their requests to the EU Cybersecurity Reserve. Receives information relating to a potential or ongoing large-scale cybersecurity incident from the cross border cyber hubs or the CSIRTs Network.	
High Representative of the Union for Foreign Affairs and Security Policy supported by the European External Action Service	Political	Leads on and coordinates the Union's efforts to address external security threats in the fields of hybrid and cyber Responsible for the Union cyber diplomacy and cyber defence instruments to deter and respond to external threats by using the Union's Hybrid and Cyber Diplomacy Toolboxes. Engages with external partners also including through CSDP engagement. Provides preparedness Union and Member States' situational awareness of and capacity to react to hybrid and cyber threats, for example through practical exercises, training and networks. Handles security and defence implications of Union space assets, especially under the Union's Common Security and Defence	Council Decision 2010/427/EU

Actor	Level	Role and competence	Reference
		Policy (CSDP). Consulted by Presidency of the Council on decisions to activate or deactivate the IPCR. EEAS develop, with the Commission services, the ISAA report.	
Europol	Operational	Provides operational and technical support to the Member States' competent authorities for the prevention and deterrence of cybercrime.	Regulation (EU) 2016/794, including all amendments
Interinstitutional Cybersecurity Board		Approves the interinstitutional cyber crisis management plan for Union entities. Adopts, based on a CERT-EU proposal, guidelines or recommendations on incident response cooperation for significant incidents concerning Union entities. .	Regulation (EU, Euratom) 2023/2841
Military Computer Emergency Response Team Operational Network (MICNET)	Technical	Foster a more robust and coordinated response to cyber threats affecting defence systems in the Union, including those used in military CSDP missions and operations; established and supported by the European Defence Agency.	Cyber Defence Joint Communication 2022
Single Intelligence Analysis Capacity (SIAC)		Composed of (1) EU Intelligence and Situation Centre (EU INTCEN) which handles civilian intelligence and open-source intelligence and provides strategic intelligence on foreign policy, terrorism, and hybrid threats, and (2) EU Military Staff Intelligence Directorate (EUMS INT) which handles military intelligence for CSDP missions and supports Union defence and crisis management operations. Under the authority of the High Representative.	Articles 38 and 42 to 46 of the Treaty on European Union Council Joint Action 2001/555/CFSP Council Decision 2010/461/CFSP

(3) Relevant Union-level crisis mechanisms

Mechanism	Horizontal/ sector/ cyber-specific	Description	Reference
ARGUS	Horizontal	Allows the Commission to exchange relevant information on emerging multisectoral crises or foreseeable or imminent threats that require Union-level action.	Commission Communication (2005)662
EEAS Crisis Response Centre (CRC)	Horizontal	The single-entry point for all crisis-related issues in the EEAS and the 24/7 permanent crisis response capability for emergencies threatening the safety of the staff in EU Delegations, and/or in reaction to crises affecting Union citizens abroad. It brings together security, consular and situational awareness experts, while relying on committed professionals on the ground in Union delegations.	A Strategic Compass for Security and Defence - For a European Union that Protects Its Citizens, Values and Interests and Contributes to International Peace and Security (21 Mach 2022)
Critical Infrastructure Blueprint	Horizontal	Coordinates a response at Union-level to disruptions to critical infrastructure with significant cross-border relevance.	Council Recommendation C/2024/4371
Cybersecurity Alert System	Cyber-specific	Ensures advanced Union capabilities to enhance detection, analysis and data processing capabilities in relation to cyber threats and the prevention of incidents in the Union.	Regulation (EU) 2025/38 (Cyber Solidarity Act) OJ L series, 15.1.2025
Cyber Diplomacy Toolbox (Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities)	Cyber-specific	The joint Union diplomatic response to malicious cyber activities, contributing to conflict prevention, the mitigation of cybersecurity threats, and greater stability in international relations.	Council Conclusions of 19 June 2017 Revised implementing guidelines 10289/23, 08.06.2023
European Cyber Reserve	Cyber-specific	Mobilises cybersecurity experts and resources during crises to support response efforts in Member States, Union institutions, bodies or	Regulation (EU) 2025/38

Mechanism	Horizontal/ sector/ cyber-specific	Description	Reference
		agencies	
Network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows	Sectoral	Establishes a recurrent process of cybersecurity risk assessments in the electricity sector, contains provisions specific to crisis management and links to the CSIRTs Network and EU-CyCLONe.	Commission Delegated Regulation (EU) 2024/1366
EU Cyber Defence Coordination Centre	Horizontal	Its initial objective is to primarily enhance the Union's and its Member States' shared situational awareness on malicious activities in cyberspace, particularly concerning military CSDP missions and operations.	Cyber Defence Joint Communication 2022
Hybrid Toolbox	Horizontal	Includes a set of provisions to ensure an overview of what is available at EU level in response to all kind of hybrid threats, their coordinated use, ensuring coherence of our actions across domains. The Hybrid Toolbox helps ensure that decision making based on a comprehensive situational awareness and the lessons learned	Council conclusions on a Framework for a coordinated EU response to hybrid campaigns, 22 June 2022
Hybrid Rapid Response Teams (EU HRRTs)	Horizontal	As part of the EU-Hybrid Toolbox, the EU Hybrid Rapid Response Teams draw on relevant sectoral national and EU civilian and military expertise to provide tailored and targeted short-term assistance to member states, Common Security and Defence Policy missions and operations, and partner countries in countering hybrid threats and campaigns.	Guiding framework for the practical establishment of the EU Hybrid Rapid Response Teams (21 May 2024)
IPCR	Horizontal	Supports rapid and coordinated decision-making at Union political level for major and complex crises, including acts of terrorism. Decision to activate and deactivate is taken by the Presidency of the Council which consults (except where in the solidarity clause has	Council Implementing Decision (EU) 2018/1993

Mechanism	Horizontal/ sector/ cyber-specific	Description	Reference
		been invoked) the affected Member States, the Commission and the HR. GSC, Commission services and EEAS may also agree, in consultation with the Presidency, to activate IPCR in information sharing mode. Discussions are informed by the ISAA report developed by Commission services and the EEAS. The report is based on relevant information and analysis provided by the Member States (e.g. from relevant national crisis centres) particularly through the web platform, and by Union Agencies	
EU Law Enforcement Emergency Response Protocol	Horizontal	A tool to support the Union law enforcement authorities in providing immediate response to major cross-border cyber-attacks through rapid assessment, the secure and timely sharing of critical information and effective coordination of the international aspects of their investigations.	Council conclusions (26 June 2018) on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises.
PESCO Cyber Rapid Response Teams (CRRT)	Cyber-specific	Deploy specialized teams to respond swiftly to significant cyber incidents as well as perform preventative actions, such as vulnerability assessments and election monitoring. Member State initiative, partly funded by Connecting Europe Facility.	Article 42 (6), Article 46 and Protocol 10 of the Treaty on European Union.
Space Threat Response Architecture (STRA)	Sectoral (Space Threats including cyber related)	Space Threat Response Architecture (STRA) on responsibilities to be exercised by the Council and the High Representative to avert a threat arising from the deployment, operation or use of the systems set up and services provided under the Union Space Programme	Council Decision (CFSP) 2021/698

Mechanism	Horizontal/ sector/ cyber-specific	Description	Reference
Systemic Cyber Incident Coordination Framework (EU-SCICF)	Sectoral	A framework which is under development for communication and coordination that addresses and manages potential systemic cyber events in the financial sector. It will build on one of the envisaged roles of the European Supervisory Authorities (ESAs) under the Regulation (EU) 2022/2554 of gradually enabling an effective Union-level coordinated response in the event of a major cross-border information and communication technologies (ICT) related incident or related threat having a systemic impact on the Union's financial sector as a whole.	Recommendation of the European Systemic Risk Board of 2 December 2021 on a pan-European systemic cyber incident coordination framework for relevant authorities (ESRB/2021/17)
Union Civil Protection Mechanism (UCPM)	Horizontal	Ensures civil protection cooperation to improve prevention, preparedness, and response to disasters.	Decision 1313/2013.
CISE - Common Information Sharing Environment	Maritime specific covering seven sectors.	CISE - is a network that connects systems of EU/EEA authorities with responsibility in maritime surveillance. CISE enables the exchange of relevant information across borders and different sectors in a seamless and automated way.	A Strategic Compass for Security and Defence - For a European Union that Protects Its Citizens, Values and Interests and Contributes to International Peace and Security (21 March 2022).

(4) Sectors of high criticality and other critical sectors under Directive (EU) 2022/2555 and Union level sectoral crisis mechanisms (where applicable)

Sectors	Subsector	Applicable sectoral crisis mechanisms
Energy	Electricity	Electricity Coordination Group
	District heating and cooling	n/a

	Oil	Oil Coordination Group The European Union Offshore Authorities Group (EUOAG)
	Gas	Gas Coordination Group
	Hydrogen	n/a
Transport	Air	European Aviation Crisis Coordination Cell (EACCC)
	Rail	n/a
	Water	European Fisheries Control Agency (EFCA) SafeSeaNet (SSN) Integrated Maritime Services (IMS) Long Range Identification and Tracking data centre (LRIT) EMSA Maritime Support Services
	Road	n/a
	Horizontal	The Network of Transport Contact Points, established by the Contingency Plan for Transport (COM(2022) 211)
Banking		EU-SCICF
Financial market infrastructures		EU-SCICF European Financial Stabilisation Mechanism

Health		Early Warning and Response System (EWRS) Health Emergency Operations Facility (HEOF) Rapid alert system for tissue and cell and blood Components (RATC/RAB) Public Health Emergency Framework Rapid Alerting System for Chemical incidents (RASCHEM) The European surveillance portal for infectious diseases Health Emergency Preparedness and Response (HERA) Medical health intelligence System (MediSys) Executive Steering Group on Shortages of Medical Devices (MDSSG) Pharmacovigilance Rapid Alert EU Health Task Force (EUHTF)
Drinking water		n/a
Waste water		n/a
Digital infrastructure		n/a
ICT service management		n/a
Public administration		n/a
Space		Space Threat Response Architecture (STRA)
Postal and courier services		n/a
Waste management		n/a
Manufacture, production and distribution of chemicals		Rapid Alerting System for Chemical incidents (RASCHEM)

Production, processing and distribution of food		European crop monitoring System Global agricultural production anomaly hotspot detection (ASAP) European Network of Plant Health Information Systems (EUROPHYT) EU Veterinary Emergency Team (EUVET) Rapid Alert System for Food and Feed (RASFF) European Food Security Crisis preparedness and response Mechanism (EFSCM) Internal Market Emergency and Resilience Act (IMERA)
Manufacturing	Medical devices	n/a
	Computer, electronic and optical products	n/a
	Machinery and equipment	n/a
	Manufacturing of motor vehicles, trailers and semi trailers	n/a
	Manufacturing of other transport equipment	n/a
Digital providers		n/a
Research		n/a

ANNEX 3 – GUIDING PRINCIPLES

The principles set out in the 2017 Cybersecurity Blueprint remain relevant.

Proportionality: most cybersecurity incidents affecting Member States fall below what could be considered a national or Union crisis. In case of cyber incidents, Member States cooperate within the CSIRTs Network and EU-CyCLONe in line with their respective procedures.

Subsidiarity: Member States have the primary responsibility for the response in case of large-scale cybersecurity incidents or crises affecting them. The Commission, the European External Action Service, ENISA, CERT-EU, Europol and all other relevant Union entities have important roles to play throughout the entire crisis life cycle. This role is set out in the IPCR arrangements but also stems from Union law and reflects how cybersecurity incidents and crises impact one or more sectors of economic activity within the single market, the security and international relations of the Union, as well as the institutions themselves.

Complementarity: this Recommendation takes fully into account existing crisis management mechanisms at Union level, namely the IPCR arrangements, ARGUS, and the EEAS Crisis Response Mechanism. It takes into account the modified roles of the CSIRTs Network and EU-CyCLONe under rules adopted since 2017 to maximise synergies and minimise duplication, and the adoption of the EU Law Enforcement Emergency Response Protocol.

Confidentiality of information: All information exchanges in the context of this Recommendation must comply with applicable rules on security, on the protection of personal data and the Traffic Light Protocol system for classifying sensitive information. For the exchange of classified information, regardless of the classification scheme applied, available accredited tools should be used. As regards the processing of personal data, the applicable Union rules, in particular are to be respected, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council[1], Directive 2002/58/EC of the European Parliament and of the Council[2], as well as Regulation (EU) 2018/1725 of the European Parliament and of the Council [3].

---

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

2 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

3 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).