EUROPEAN
COMMISSION

Brussels, 23.6.2026
COM(2026) 314 final

2026/0173 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulation (EU) 2018/1725 of the European Parliament and of the Council 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

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices and agencies (EUDPR) was designed to establish a coherent and modernised data protection regime for all EU institutions, bodies, offices, and agencies. Chapter IX of Regulation (EU) 2018/1725 was specifically intended to govern the processing of 'operational personal data' (that is the personal data processed for carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU) by EU Justice and Home Affairs (JHA) agencies and bodies, including Europol, Eurojust, the European Public Prosecutor's Office (EPPO), and, to a limited extent, Frontex.

Notwithstanding the adoption of the EUDPR, the data protection framework applicable to EU JHA agencies and bodies remains fragmented. In particular, Chapter IX does not apply to the EPPO, whose founding Regulation predates the EUDPR. As a result, certain provisions of the EPPO Regulation diverge in substance from, or are formulated differently than the corresponding provisions set out in Chapter IX of the EUDPR. Furthermore, the EUDPR provides that, with respect to the processing of operational personal data, only Article 3 (definitions) and Chapter IX are applicable. On the one hand, this has resulted in retaining provisions regulating certain aspects relating to processing of operational personal data in founding acts of the respective bodies, offices or agencies. On the other hand, it has given rise to legal uncertainty as to whether, and to what extent, provisions contained in Chapter II to VIII such as those relating to records of processing activities or the data protection officer's tasks apply in situations where analogous provisions do not exist either in Chapter IX or in the founding acts of the relevant bodies, offices or agencies. This fragmentation not only undermines legal certainty but also creates practical obstacles to effective cooperation between EU bodies, offices and agencies when sharing data. In its first EUDPR application report of 2022, the Commission acknowledged these shortcomings and considered legislative intervention to address them.

In this context, the present proposal pursues the objectives of simplification and ensuring consistency of the applicable data protection framework, notably by aligning the relevant rules across EU bodies and agencies. This alignment is expected to alleviate administrative burdens and facilitate data exchanges between them, while at the same time enhancing legal certainty. In the interest of consistency and in line with the general objective of minimising the fragmentation of data protection rules the proposal rests upon four primary objectives:

Ensuring consistent application of data protection to all EU institutions, bodies, offices and agencies

Chapter IX needs to have an extended scope to ensure it applies consistently across all EU agencies, bodies and offices in the criminal justice and law enforcement sector. It will integrate the EPPO into the EUDPR framework. This will be done without prejudice to the possibility to keep, in the EPPO Regulation, the specific data protection rules needed to reflect the unique nature of the EPPO as the independent public prosecutor's office of the Union. The rules in Chapter IX are already aligned with the corresponding rules of the Law Enforcement Directive (EU) 2016/680 and will result in a single, harmonised set of rules for all affected parties to reduce fragmentation and ensure consistency of rules applied.

Enhancing legal certainty

At present, Chapter IX lacks provisions on several important aspects, including the role of Data Protection Officers (DPOs), the maintenance of records of processing activities, collaboration between supervisory authorities, and the international transfer of operational personal data. The proposal aims to consolidate the rules in one place, streamlining compliance without imposing a significant operational impact. This will also provide greater clarity for controllers, processors, and data subjects.

Streamlining the powers of the European Data Protection Supervisor

Currently, the EDPS's supervisory powers are regulated in founding acts of Europol, Eurojust and the EPPO, each containing divergent provisions, leading to uncertainty and inefficiencies. The founding act of Frontex does not regulate the EDPS supervision for processing operational data, resulting in an important asymmetry.

The proposal seeks to clarify that the EDPS is granted supervisory powers which are in line with those under Article 58 EUDPR, however adapted to the context of processing operational data, notably for the EPPO in the context of investigation and prosecution activities. In that respect, the proposal follows the model for EDPS powers from 2022 Europol reform, while ensuring consistency with Chapter VI of the EUDPR and the Law Enforcement Directive (LED). The proposal removes agency-specific provisions on EDPS tasks and powers from founding acts.

General streamlining

Finally, the proposal aims to streamline provisions to eliminate redundancies, duplications and inconsistencies in the area of data protection for JHA Union bodies, offices and agencies when carrying out the activities falling within the scope of Chapter 4 and 5 of Title V of Part Three TFEU. It also aligns the provisions on processing of operational data with the Digital Omnibus proposal[(1)], when relevant.

- **Consistency with existing policy provisions in the policy area**

The proposal aims to align the provisions of the EUDPR with existing data protection policies, reinforcing the principles established in the General Data Protection Regulation (GDPR) and the LED. It ensures alignment with amendments to data protection framework proposed under Digital Omnibus, when relevant.

- **Consistency with other Union policies**

The proposal is part of a package of criminal justice initiatives pursuing a coherent and complementary objective: strengthening the Union’s capacity to prevent, detect, investigate and prosecute serious cross-border crime in an increasingly complex security environment. By modernising the legal frameworks governing cooperation between law enforcement, judicial and other relevant authorities, the package seeks to reinforce the effectiveness, coherence and interoperability of the Union’s internal security architecture.

The proposed revisions of the Europol and Eurojust Regulations constitute the core of this effort. Europol and Eurojust perform distinct yet complementary functions within the Area of Freedom, Security and Justice: while Europol supports the prevention, detection and investigation of criminal activities, Eurojust facilitates judicial cooperation and ensures effective prosecutorial and judicial follow-up. The package therefore aims to strengthen

(1) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), 19.11.2025, COM(2025)837 final.

cooperation and complementarity between the two agencies, as well as with other relevant Union actors in the Justice and Home Affairs and Anti-Fraud Architecture (AFA) areas, with a view to ensuring a seamless continuum between law enforcement action and judicial follow-up across all stages of the criminal justice chain.

In this context, the amendments to the European Investigation Order framework and the present proposal further contribute to this objective by facilitating effective cross-border cooperation, improving the conditions for information exchange and ensuring a coherent legal framework adapted to operational realities and technological developments. Taken together, the measures proposed in this package will enhance the Union's ability to respond to evolving security threats while fully respecting fundamental rights, the rule of law and the division of responsibilities between the different actors involved.

In particular, this proposal identifies all common denominators of data protection rules applicable to Europol and Eurojust, and regroups them in the EUDPR, thereby removing fragmentation and duplication. This allows the founding acts of Union bodies, offices and agencies active in the area of law enforcement and criminal justice to maintain only those tailored-made data protection rules, developed to reflect their respective specific operational needs and nature.

The proposal is adopted in parallel with the revisions of the Europol and Eurojust Regulations, ensuring coherence and alignment across the respective legal frameworks. It also anticipates the forthcoming revision of the EPPO founding act Regulation (EU) 2017/1939[(2)], taking into consideration its future developments and without prejudice to the assessment of the possible policy options for the revision of the EPPO Regulation. This coordinated approach contributes to a comprehensive and consistent framework for processing operational data by Union bodies and agencies.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The protection of natural persons in relation to the processing of their personal data is a fundamental right laid down in Article 8(1) of the Charter of Fundamental Rights of the European Union.

This proposal is based on Article 16 TFEU, which is the legal basis for adopting data protection rules. This Article allows for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies when carrying out activities which fall within the scope of Union law. It also allows for the adoption of rules relating to the free movement of personal data, including personal data processed by those institutions, bodies, offices and agencies.

• Subsidiarity (for non-exclusive competence)

Not Applicable

• Proportionality

Not Applicable

• Choice of the instrument

Not Applicable

(2) Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') (OJ L 283, 31.10.2017, pp. 1–71, ELI: http://data.europa.eu/eli/reg/2017/1939/oj)

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

• Ex-post evaluations/fitness checks of existing legislation

The Commission's 2022 first EUDPR application report concluded that, overall, the EUDPR is working well and is fit for purpose. At the same time, it identified the need for legislative intervention to minimise the fragmentation of data protection rules for EU institutions and bodies processing operational personal data when carrying out activities in the scope of police cooperation and judicial cooperation in criminal matters (Chapter IX of the EUDPR, the 'law enforcement chapter').

• Stakeholder consultations

Targeted stakeholder consultations were carried out with all the entities currently or subject in the future to Chapter IX EUDPR (i.e. Europol, Eurojust, the EPPO, Frontex) as well as the European Data Protection Supervisor, which is in charge of overseeing compliance.

• Collection and use of expertise

Not Applicable

• Impact assessment

An impact assessment is not considered appropriate for this initiative due to its limited scope and largely technical nature of the proposed amendments. The proposal targets specific provisions of the EUDPR, affecting only a small group of EU entities in the field of judicial cooperation in criminal matters and police cooperation, without altering the overall framework. The changes aim at ensuring a better harmonised regime and do not involve new policy options, and are expected to have minimal, non-quantifiable impact on fundamental rights, and no economic, social, or environmental, implications. Additionally, the relevant agencies are already subject to separate evaluations and impact assessments including with regard to the data protection rules applicable to them. A separate assessment under the EUDPR would duplicate this exercise. The proposal aligns with the prior commitment of the Commission in its first EUDPR application report of 2022 and a further evaluation of the EUDPR is envisaged in 2027. Finally, subsidiarity concerns do not arise, as the EUDPR applies exclusively to EU bodies, which cannot be regulated by Member States.

• Regulatory fitness and simplification

The proposal harmonises and simplifies the data protection rules applicable to Union agencies, offices and bodies active in the area of criminal law enforcement and criminal justice. By streamlining existing rules, it enhances legal clarity and consistency across the institutional framework, thereby facilitating their application and reducing administrative complexity. While the benefits are not readily quantifiable, the proposal is expected to lower compliance costs and administrative burdens associated with navigating different or overlapping requirements. The proposal also supports the development of any inter-actor exchange mechanism considered in the context of the Anti-Fraud Architecture review.

• Fundamental rights

The targeted nature of the changes ensures that existing level of data protection is maintained, while providing for improvements as regards consistency of applicable rules and further harmonisation.

4. BUDGETARY IMPLICATIONS

Not Applicable

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

Not Applicable

- **Detailed explanation of the specific provisions of the proposal**

Article 1 covers amendments to Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices and agencies.

Paragraph (1) replaces paragraph 2 of Article 2 and broadens the scope of application of Articles 43, 44, 45, and Chapters VII and VIII of Regulation (EU) 2018/1725 to the processing of operational personal data by Union bodies, offices and agencies, without prejudice to specific data protection rules applicable to Union bodies, offices or agencies. It also deletes paragraph 3 of Article 2, thereby extending the application of the EUDPR to the EPPO, without however undermining the need to retain, in the EPPO Regulation, specific data protection rules that account for the EPPO's distinct nature as the independent investigative and prosecutorial authority of the Union.

Paragraph (2) provides for technical adjustments to the wording of Article 45 on tasks of the Data Protection Officer, and ensures that said tasks cover also processing of operational data.

Paragraph (3) ensures that the European Data Protection Supervisor’s power under Article 66 of Regulation (EU) 2018/1725 to impose administrative fines extends to the processing of operational personal data by Union bodies, offices and agencies.

Paragraph (4) deletes Article 70 of Regulation (EU) 2018/1725, which is obsolete in light of defining the provisions applicable to the processing of operational data in Article 2(2).

Paragraph (5) amends Article 77 of Regulation (EU) 2018/1725 to ensure alignment with the Digital Omnibus proposal and to enhance legal certainty, by specifying that decisions based solely on the automated processing of operational personal data are permissible where specific conditions are satisfied.

Paragraph (6) amends Article 78 of Regulation (EU) 2018/1725 to ensure alignment with the Digital Omnibus proposal by clarifying the notion of abusive requests in the context of the right of access. In particular, it specifies that a request may be considered manifestly unfounded where the data subject relies on the right of access for purposes other than the protection of their data. In such cases, the controller may refuse to act on the request, while remaining subject to the obligation to demonstrate that the request is manifestly unfounded or excessive.

Paragraph (7) introduces a new Article 87a in Regulation (EU) 2018/1725 on record-keeping for operational personal data, in alignment with the rules of the LED.

Paragraphs (8) and (9) add additional safeguards to Article 88 of Regulation (EU) 2018/1725 on logging.

Paragraph (10) amends Article 92(1) of Regulation (EU) 2018/1725 to ensure alignment with the Digital Omnibus proposal by extending the deadline for notifying a personal data breach to the European Data Protection Supervisor from 72 hours to 96 hours. It also raises

the notification threshold by providing that notification is required only where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

Paragraphs (11) and (12) streamline the legal framework governing transfers of operational personal data to third countries and international organisations, by aligning them with framework set up in Directive (EU) 2016/680. The amendments provide a uniform set of rules applicable to Union bodies, offices and agencies active in area of the criminal law enforcement and criminal justice, while taking into account their specific operational and legal context, including cooperation agreements. They provide that transfers to countries with an adequacy decision are permitted without further authorisation; in the absence of an adequacy decision, transfers are allowed if appropriate safeguards are in place through a legally binding instrument, or a controller's assessment; and in specific scenarios where neither an adequacy decision nor appropriate safeguards exist, certain derogations apply. Finally, they also provide for transfers of operational personal data to recipients who are not competent authorities established in third countries in specific cases provided that the conditions listed therein are met, including when contacting a competent authority in third country may be ineffective or inappropriate and that the transfer is strictly necessary for the performance of the controller's tasks.

Paragraph (13) streamlines the powers of the European Data Protection Supervisor for operational personal data for all Union bodies, offices and agencies active in the area of criminal law enforcement and criminal justice, in line with the powers of the European Data Protection Supervisor applicable to Europol as of 2022.

Article 2 clarifies when new provisions enter into force.

2026/0173 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulation (EU) 2018/1725 of the European Parliament and of the Council 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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national Parliaments,

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her. This right is also guaranteed under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(2) Regulation (EU) 2018/1725 of the European Parliament and of the Council [(1)] establishes the legal framework for the processing of personal data by Union institutions, bodies, offices and agencies. However, the data protection rules on the processing of operational personal data of by Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU remain laid down in a fragmented manner between Chapter IX of Regulation (EU) 2018/17/25 and other Union legal acts. Article 98 of that Regulation requires the Commission to review the rules applicable to the processing of operational personal data, with a view to identifying possible inconsistencies, gaps and divergences. It also provides that the Commission, where appropriate, addresses identified shortcomings by a legislative proposal, in particular to extend the application of Chapter IX to the European Public Prosecutor's Office (EPPO) established by Council Regulation (EU) 2017/1939[(2)], as appropriate, and to introduce the necessary adaptations to that Chapter. In its first application report on the Regulation (EU) 2018/1725, the Commission confirmed the Regulation's overall

[(1)] 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).

[(2)] Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') (OJ L 283, 31.10.2017, p. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj).

effectiveness in ensuring a high level of protection of personal data, while highlighting a number of inconsistencies, divergencies and legal fragmentation arising from the interplay between Chapter IX and the other provisions of Regulation (EU) 2018/1725, as well as the existence of a standalone data protection regime for the EPPO.

(3) Currently, only Article 3 and Chapter IX of Regulation (EU) 2018/1725 apply to the processing of operational personal data, together with a number of specific data protection rules laid down in the founding acts of the European Union Agency for Law Enforcement Cooperation (Europol) and the European Union Agency for Criminal Justice Cooperation (Eurojust). At the same time, the EPPO has its own, standalone data protection regime in its founding act. Therefore, Regulation (EU) 2018/1725 should be amended in order to extend the application of its Chapter IX to all Union bodies, offices and agencies processing operational personal data in the law enforcement and criminal justice sector, to ensure legal certainty by addressing gaps in the current data protection regime, in particular for the European Border and Coast Guard Agency and to streamline the rules on international transfers of personal data, as well as the rules on the powers of the European Data Protection Supervisor. That should not affect the possibility to keep, in Regulation (EU) 2017/1939, the specific data protection rules needed to reflect the unique nature of the EPPO as the independent public prosecutor's office of the Union.

(4) In order to create a harmonised, consistent, simplified and complete legal framework for processing of operational personal data by Union bodies, offices and agencies, the definitions (Chapter I), the rules on data protection officers (Section 6 of Chapter IV), the rules on cooperation and consistency (Chapter VII), the rules on remedies, liability and penalties (Chapter VIII) and the rules on processing of operational personal data (which should be aligned with Directive (EU) 2016/680 of the European Parliament and of the Council[3] – Chapter IX) laid down in Regulation (EU) 2018/1725 should apply to Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU. Those rules should apply where they exercise such activities for the purposes of the prevention, detection, investigation or prosecution of criminal offences. Those rules, , should also apply to the processing of operational personal data by the European Border and Coast Guard Agency, rather than only Chapter IX of Regulation (EU) 2018/1725. The rules of Regulation (EU) 2018/1725 should apply without affecting the specific rules applicable to the processing of operational personal data by Union bodies, offices and agencies when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU, in particular the rules laid down in the founding acts of Europol, Eurojust and EPPO. Such specific rules should be regarded as *lex specialis* to the provisions of Regulation (EU) 2018/1725 on the processing of operational personal data.

(5) A data protection officer within all Union institutions and bodies should ensure that all data protection rules, including Regulation (EU) 2018/1725 are applied. Officers should also advise controllers and processors as to their obligations. In order to ensure

[3] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

consistency and prevent duplication, in matters of both administrative and operational personal data, there should be only one set of rules for data protection officers.

(6) The European Data Protection Supervisor should, as a measure of last resort, have the power to impose administrative fines, including for processing of operational personal data by Union bodies, offices and agencies active in the area of law enforcement and criminal justice.

(7) In order to avoid duplication within Regulation (EU) 2018/1725, Article 70 thereof should be deleted, as the scope of Chapter IX is already regulated in Article 2 of Regulation (EU) 2018/1725.

(8) In order to ensure the alignment with Regulation (EU) …/… [*the Digital Omnibus proposal*], it should be clarified in Article 77 of Regulation (EU) 2018/1725 that decisions based solely on automated processing of operational personal data are allowed when specific conditions are met.

(9) In order to ensure the alignment with Regulation (EU) …/… [*the Digital Omnnibus proposal*], it should be clarified in Article 78 of Regulation (EU) 2018/1725 that the right of access, which is from the outset favourable to data subjects, should not be abused in the sense that the data subjects abuse them for purposes other than the protection of their data.

(10) In order to demonstrate compliance with Regulation (EU) 2018/1725, Union bodies, offices and agencies active in the area of law enforcement and criminal justice should have uniform rules on maintaining records regarding all categories of processing activities under their responsibility. Each controller and processor should be obliged to cooperate with the European Data Protection Supervisor and make those records available to it on request, so that they might serve for monitoring those processing operations.

(11) Union bodies, offices and agencies should not be able to modify logs. Where Union bodies, offices and agencies receive operational personal data from national competent authorities, the Union bodies, offices and agencies should communicate the logs to those authorities, when they are necessary for internal data protection compliance investigations.

(12) In order to ensure the alignment with Regulation (EU) …/… [*the Digital Omnibus proposal*], the threshold should be higher and a deadline should be prolonged, for notifying a personal data breach to the European Data Protection Supervisor.

(13) Union bodies, offices and agencies active in the area of law enforcement and criminal justice should all benefit from a uniform set of rules on international transfers of operational personal data, aligned with Directive (EU) 2016/680.

(14) The Commission may decide, under Article 36 of Directive (EU) 2016/680, that a third country, a territory or specified sector within a third country or an international organisation offers an adequate level of data protection. In such cases, transfers of operational personal data to that third country or international organisation by Union bodies, offices and agencies can take place without the need to obtain any further authorisation.

(15) Transfers not based on such an adequacy decision should be allowed only where appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or where the controller has assessed all the circumstances surrounding the data transfer and, on the basis of that assessment,

considers that appropriate safeguards with regard to the protection of personal data exist. Such legally binding instruments could, for example, be cooperation agreements between Eurojust and a third country concluded before 12 December 2019 in accordance with Article 26a of Decision 2002/187/JHA, cooperation agreements between Europol and a third country concluded before 1 May 2017 in accordance with Article 23 of Decision 2009/371/JHA, or international agreements concluded between the Union and a third country pursuant to Article 218 TFEU.

(16) Where no adequacy decision or appropriate safeguards exist, a transfer or a category of transfers could take place by derogation in specific situations. Derogations should be interpreted restrictively and should not allow frequent, massive and structural transfers of personal data, or large-scale transfers of data, but should be limited to strictly necessary data. Such transfers should be documented and should be made available to the European Data Protection Supervisor on request in order to monitor the lawfulness of the transfer.

(17) In specific individual cases, the regular procedures requiring contacting a competent authority in a third country may be ineffective or inappropriate, in particular because the transfer could not be carried out in a timely manner, or because that authority in the third country does not respect the rule of law or international human rights norms and standards. This may be the case where there is an urgent need to transfer personal data to a private company in a third country in order to receive information about an unknown perpetrator of an online crime, or to save the life of a person who is in danger of becoming a victim of a criminal offence, or in the interest of preventing an imminent perpetration of a crime, including terrorism. In such cases, under specific conditions, Union bodies, offices and agencies could decide to transfer operational personal data directly to recipients which are not competent authorities, established in those third countries.

(18) The European Data Protection Supervisor should have a uniform set of powers applicable to the processing of operational personal data by Union bodies, offices and agencies active in the area of law enforcement and criminal justice. Such powers have already been applicable to Europol since 2022, for example, ordering the data controller to ensure compliance with Regulation (EU) 2018/1725, ordering the suspension of data flows to a recipient in a Member State, a third country or an international organisation, or imposing an administrative fine in the case of non-compliance by its order.

(19) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered its opinion on XX XX 2026.

HAVE ADOPTED THIS REGULATION:

Article 1

Amendments to Regulation (EU) 2018/1725

Regulation (EU) 2018/1725 is amended as follows:

1. Article 2 is amended as follows:

(a) paragraph 2 is replaced by the following:

'2. Only Articles 3, 43, 44, 45 and Chapters VII, VIII and IX of this Regulation shall apply to the processing of operational personal data by Union bodies, offices and agencies when carrying out activities which fall within the scope of

Chapter 4 or Chapter 5 of Title V of Part Three TFEUs, without affecting specific data protection rules applicable to such a Union body, office or agency.'

(b) paragraph 3 is deleted;

2. in Article 45(1), points d), e) and (f) are replaced by the following:

‘ d) to provide advice where requested as regards the necessity for a notification or a communication of a personal data breach pursuant to Articles 34 and 35, or Articles 92 and 93;

e) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 39 or Article 89 and to consult the European Data Protection Supervisor in case of doubt as to the need for a data protection impact assessment;

f) to provide advice where requested as regards the need for prior consultation of the European Data Protection Supervisor pursuant to Article 40 or Article 90; to consult the European Data Protection Supervisor in case of doubt as to the need for a prior consultation;'

3. in Article 66(1), the first sentence is replaced by the following:

‘1. The European Data Protection Supervisor may impose administrative fines on Union institutions and bodies, depending on the circumstances of each individual case, where a Union institution or body fails to comply with an order by the European Data Protection Supervisor pursuant to Article 58(2), points (d) to (h) and (j), or pursuant to Article 95a(3), points (c), (e), (f), (j) and (k).’

4. Article 70 is deleted.

5. In Article 77, paragraph 1 is replaced by the following:

‘1. A decision which produces legal effects for a data subject or similarly significantly affects him or her may be based solely on automated processing, including profiling, only where that decision is authorised by Union law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller.’

6. Iin Article 78, paragraph 4 is replaced by the following:

‘4. The controller shall provide the information under Article 79 and any communication made or action taken pursuant to Articles 80 to 84 and 92 free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or, for requests under Article 80 where the data subject abuses the right of access for purposes other than the protection of their data, the controller may refuse to act on the request. The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive.’

7. the following Article 87a is inserted:

‘Article 87a

Records of categories of processing activities of operational personal data

1. Each controller shall maintain a record of all categories of processing activities of operational personal data under its responsibility. That record shall contain all of the following information:

(a) the controller's contact details and the name and the contact details of the Data Protection Officer, and, where applicable, the contact details of the joint controller;

(b) the purposes of the processing;

(c) the categories of recipients to whom the personal data have been or will be disclosed including private parties, and recipients in third countries or international organisations;

(d) a description of the categories of data subjects and of the categories of personal data;

(e) where applicable, the use of profiling;

(f) where applicable, the categories of transfers of personal data to a private party, a third country or an international organisation;

(g) an indication of the legal basis for the processing operation, including transfers, for which the personal data are intended;

(h) where possible, the envisaged time limits for erasure of the different categories of data;

(i) where possible, a general description of the technical and organisational security measures referred to in Article 91(1).

2. The processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the processor's or processors' contact details, of each controller on behalf of which the processor is acting and the contact details of the Data Protection Officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a private party, a third country or an international organisation where explicitly instructed to do so by the controller, including the identification of that third country or international organisation;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 91(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form. The controller and the processor shall make those records available to the European Data Protection Supervisor on request.'

8. in Article 88(1), the following sentence is added:

'It shall not be possible to modify logs.'

9. in Article 88(3), the following sentence is added:

'If required by the national competent authority for a specific investigation related to compliance with data protection rules, the logs referred to in paragraph 1 shall be communicated to that authority.'

10. In Article 92, paragraph 1 is replaced by the following:

‘1. In the case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall without undue delay and, where feasible, not later than 96 hours after having become aware of it, notify the personal data breach to the European Data Protection Supervisor. Where the notification to the European Data Protection Supervisor is not made within 96 hours, it shall be accompanied by reasons for the delay.’

11. Article 94 is replaced by the following:

'Article 94

General principles for transfers of operational personal data to third countries and international organisations

1. The controller may transfer operational personal data to a third country or to an international organisation, subject to compliance with the applicable data protection rules and the other provisions of this Regulation, and only where the following conditions are met:

(a) the transfer is necessary for the performance of the controller’s tasks;

(b) the authority of the third country or the international organisation to which the operational personal data are transferred is competent in law enforcement or criminal justice matters;

(c) where the operational personal data to be transferred have been transmitted or made available to the controller by a Member State or Union body, office and agency, the controller shall obtain prior authorisation for the transfer from the relevant competent authority of that Member State or from the Union body, office and agency in compliance with its applicable law, unless that Member State or Union body, office and agency has authorised such transfers in general terms or subject to specific conditions;

(d) in the case of an onward transfer to another third country or international organisation by a third country or international organisation, the controller shall require the transferring third country or international organisation to obtain the prior authorisation of the controller for that onward transfer;

(e) the controller shall only provide authorisation under point (d) with the prior authorisation of the Member State or the Union body, office and agency from which the data originate, where applicable, after taking due account of all relevant factors, including the seriousness of the criminal offence, the purpose for which the operational personal data were originally transferred and the level of personal data protection in the third country or international organisation to which the operational personal data are to be transferred onward.

2. Subject to the conditions set out in paragraph 1 of this Article, the controller may transfer operational personal data to a third country or to an international organisation where the conditions of Articles 94a, 94b, 94c or 94d are fulfilled.

3. Without affecting Article 94c, the controller may transfer operational personal data to a competent authority of a country associated with the implementation, application and development of the Schengen *acquis* that has implemented and effectively applies the provisions of Directive (EU) 2016/680, and the provisions on the exchange of information laid down in Directive (EU) 2023/977.

4. The controller may in urgent cases transfer operational personal data without prior authorisation from a Member State or Union body, office and agency in accordance with paragraph 1, point (c). The controller shall only do so if the transfer of the operational personal data is necessary for the prevention of an immediate and serious threat to the public security of a Member State or of a third country or to the essential interests of a Member State, and where the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.

5. All provisions on international transfers in this Chapter shall be applied in order to ensure that the level of protection of natural persons ensured by this Regulation is not undermined.'

12. the following articles are inserted:

'Article 94a

Transfers on the basis of an adequacy decision

The controller may transfer operational personal data to a third country or to an international organisation where the Commission has decided in accordance with Article 36 of Directive (EU) 2016/680 that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.

Article 94b

Transfers subject to appropriate safeguards

1. In the absence of an adequacy decision, the controller may transfer operational personal data to a third country or an international organisation where:

(a) appropriate safeguards with regard to the protection of operational personal data are provided for in a legally binding instrument;

(b) or the controller has assessed all the circumstances surrounding the transfer of operational personal data and has concluded that appropriate safeguards exist with regard to the protection of operational personal data.

2. The legally binding instrument under paragraph 1, point (a) shall be:

(a) an international agreement between the Union and the third country or international organisation pursuant to Article 218 TFEU that provides for adequate safeguards with respect to the protection of privacy, data protection and other fundamental rights and freedoms of individuals;

(b) a cooperation agreement allowing for the exchange of operational personal data concluded before 12 December 2019 between Eurojust and that third country or international organisation, in accordance with Article 26a of Decision 2002/187/JHA; or

(c) a cooperation agreement allowing for the exchange of operational personal data concluded before 1 May 2017 between Europol and that third country or international organisation in accordance with Article 23 of Decision 2009/371/JHA.

3. Union bodies, offices and agencies may enter into working arrangements to set out modalities to implement the agreements referred to in paragraph 2.

4. The controller shall inform the European Data Protection Supervisor about categories of transfers under paragraph 1, point (b).

5. When a transfer is based on paragraph 1, point (b), such a transfer shall be documented and the documentation shall be made available to the European Data Protection Supervisor on request. The documentation shall include a record of the date and time of the transfer and information about the receiving competent authority, about the justification for the transfer and about the operational personal data transferred.

Article 94c

Derogations for specific situations

1. In the absence of an adequacy decision, or of appropriate safeguards pursuant to Article 94b, the controller may transfer operational personal data to a third country or an international organisation only on the condition that the transfer is necessary:

(a) in order to protect the vital interests of the data subject or another person;

(b) to safeguard legitimate interests of the data subject;

(c) for the prevention of an immediate and serious threat to public security of a Member State or a third country;

(d) or in individual cases, for the performance of the tasks of the controller, unless the controller determines that the fundamental rights and freedoms of the data subject concerned override the public interest in the transfer.

2. Where a transfer is based on paragraph 1, such a transfer shall be documented and the documentation shall be made available to the European Data Protection Supervisor on request. The documentation shall include a record of the date and time of the transfer, and information about the receiving competent authority, about the justification for the transfer and about the operational personal data transferred.

Article 94d

Transfer of operational personal data to recipients established in third countries

1. By way of derogation from Article 94(1), point (b), and without affecting any international agreement referred to in paragraph 2 of this Article, the controller, in individual and specific cases, may transfer operational personal data directly to recipients established in third countries only if all of the following conditions are fulfilled:

(a) the transfer is strictly necessary for the performance of the controller’s tasks, for the purposes for which is allowed to process operational personal data;

(b) the controller determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand;

(c) the controller considers that the transfer to a competent authority in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time;

(d) the competent authority in the third country is informed without undue delay, unless this is ineffective or inappropriate;

(e) the controller informs the recipient of the specified purpose or purposes for which the operational personal data are only to be processed by the latter provided that such processing is necessary.

2. An international agreement referred to in paragraph 1 shall be any bilateral or multilateral international agreement in force between the Union and third countries in the field of judicial cooperation in criminal matters and police cooperation.

3. Where a transfer is based on paragraph 1, such a transfer shall be documented and the documentation shall be made available to the European Data Protection Supervisor on request, including the date and time of the transfer, and information about the receiving competent authority, about the justification for the transfer and about the operational personal data transferred.'

13. the following Article 95a is inserted:

'Article 95a

Supervision by the European Data Protection Supervisor

1. The European Data Protection Supervisor shall be responsible for monitoring and ensuring the application of the provisions relating to the protection of fundamental rights and freedoms of natural persons with regard to the processing of operational personal data by Union bodies, offices and agencies, and for advising them and data subjects on all matters concerning the processing of operational personal data. To that end, he or she shall fulfil the duties set out in paragraph 2 and exercise the powers laid down in paragraph 3, while closely cooperating with the national supervisory authorities.

2. The European Data Protection Supervisor shall have the following duties:

(a) hearing and investigating complaints, and informing the data subject of the outcome within a reasonable period; conducting inquiries either on his or her own initiative or on the basis of a complaint, and informing the data subject of the outcome within a reasonable period;

(b) monitoring and ensuring the application of this Regulation and any other Union act relating to the protection of natural persons with regard to the processing of operational personal data by Union bodies, offices and agencies;

(c) advising Union bodies, offices and agencies, either on his or her own initiative or in response to a consultation, on all matters concerning the processing of operational personal data, in particular before they draw up internal rules relating to the protection of fundamental rights and freedoms with regard to the processing of operational personal data;

(d) keeping a register of new types of processing operations notified to him or her;

(e) carrying out a prior consultation on processing notified to him or her.

3. The European Data Protection Supervisor may pursuant to this Regulation:

(a) give advice to data subjects on the exercise of their rights;

(b) refer a matter to the Union body, office and agency in the event of an alleged breach of the provisions governing the processing of operational personal data, and, where appropriate, make proposals for remedying that breach and for improving the protection of the data subjects;

(c) order that requests to exercise certain rights in relation to operational personal data be complied with where such requests have been refused in breach of the applicable rules on data subject rights;

(d) warn or admonish the Union body, office or agency;

(e) order the Union body, office or agency to carry out the rectification, restriction, erasure or destruction of personal data which have been processed in breach of the provisions governing the processing of operational personal data and to notify such actions to third parties to whom such data have been disclosed;

(f) impose a temporary or definitive ban on processing operations by the Union body, office or agency which are in breach of the provisions governing the processing of operational personal data;

(g) refer a matter to the Union body, office or agency and, if necessary, to the European Parliament, the Council and the Commission;

(h) refer a matter to the Court of Justice of the European Union under the conditions provided for in the TFEU;

(i) intervene in actions brought before the Court of Justice of the European Union;

(j) order the controller or processor to bring processing operations into compliance with this Regulation and, where applicable, with data protection rules laid down in the founding act of the Union body, office or agency, where appropriate, in a specified manner and within a specified period;

(k) order the suspension of data flows to a recipient in a Member State, a third country or to an international organisation;

(l) impose an administrative fine under Article 66 in the case of non-compliance by the Union body, office and agency with one of the measures referred to in points (c), (e), (f), (j) and (k) of this paragraph, depending on the circumstances of each individual case.

4. The European Data Protection Supervisor shall have the power to:

(a) obtain from the Union body, office and agency access to all operational personal data and to all information necessary for his or her enquiries;

(b) obtain access to any premises in which the Union body, office or agency carries on its activities when there are reasonable grounds for presuming that an activity covered by this Chapter is being carried out there.

5. The European Data Protection Supervisor shall prepare an annual report on his or her supervisory activities in relation to the controllers under this Chapter. That report shall be part of the annual report of the European Data Protection Supervisor referred to in Article 60.

The EDPS shall invite the national supervisory authorities to submit observations on that part of the annual report before the annual report is adopted. The EDPS shall take utmost account of those observations and shall refer to them in the annual report.

The part of the annual report referred to in the second subparagraph shall include statistical information regarding complaints, inquiries, and investigations, as well as regarding transfers of operational personal data to third countries and international

organisations, cases of prior consultation of the European Data Protection Supervisor, and the use of the powers laid down in paragraph 3 of this Article.

6. The European Data Protection Supervisor, the officials and the other staff members of the European Data Protection Supervisor's Secretariat shall be bound by the obligation of confidentiality, in accordance with Article 95.'

Article 2

Entry into force

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. However, this Regulation shall apply to processing of operational personal data by the European Public Prosecutors' Office from [*day of entry into application of the new EPPO Regulation*].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*
[...]	*[...]*