DIGITALEUROPE

1 SEPTEMBER 2023

Squaring GDPR enforcement: stronger procedures for the one-stop shop

Executive summary

DIGITALEUROPE welcomes the proposed Regulation laying down additional procedural rules for the enforcement of the General Data Protection Regulation (GDPR).[1]

The proposal is an opportunity to reinforce the one-stop-shop (OSS) mechanism, which is central to the Digital Single Market. As is the proposal's intention, this can be done by complementing, without reopening, the GDPR.

In line with the proposal's ambition and for increased efficacy, we suggest:

- Further specifying the framework for **amicable settlements** throughout cross-border cases, after complaints or in ex-officio cases;
- Reinforcing safeguards for highly **confidential information and trade secrets** in the summary of key issues and administrative files;
- Ensuring that the parties' positions are **heard throughout the proceedings**, including in dispute resolution mechanisms;
- Setting **procedural deadlines** that fully safeguard due process, notably in the timeframe to provide a response to the administrative file shared; and
- Avoiding disproportionate limits to the lead supervisory authority's (LSA) responsibility in establishing the **scope of its own investigations**.

[1] COM(2023) 348 final and Regulation (EU) 2016/679, respectively.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Table of contents

Complaints submission and handling

Company complaint mechanisms

To ensure outcome-based enforcement, we recommend that in their assessment of the extent to which a complaint should be investigated, data protection authorities (DPAs) verify the complainant's reasonable use of the company's complaint mechanisms. Companies may offer several suitable options to make a complaint, so as to reach amicable resolutions at an early stage. This should therefore be listed in the proposal's Art. 4 and its Annex.

Amicable case resolution

We welcome the inclusion of a framework for amicable settlements in the proposal, giving the legal tool firmer ground after its recognition both in Recital 131 GDPR and in EDPB Guidelines 06/2022.

Non-litigious agreements between complainants and parties under investigation must be encouraged, so as to allow for speedier, less costly procedures for the parties and for DPAs.

However, Art. 5 remains limited, as for instance the role of the LSA in amicable settlements is not detailed. The possibility of amicable decisions in ex-officio cases, which could allow parties to reach a common understanding, is not specified either.

Overall, we urge that amicable settlements should be possible at all stages of cross-border procedures. Where a solution emerges, parties should have the option to form an agreement on common terms at all stages of the procedure.

Cooperation procedure and the OSS mechanism

The proposed Regulation, as presently drafted, shifts several competences and responsibilities from the LSA to other concerned supervisory authorities (CSAs), in the 'cooperation procedure.'

For instance, where there is no consensus between the LSA and one or more CSAs on the LSA's preliminary identification of the scope of the investigation, the European Data Protection Board (EDPB) can adopt an urgent binding decision within two weeks by simple majority.

Rather than making the OSS more efficient, this early accelerated procedure could result in an increase in dispute resolution requests. Instead, the final text should reflect that Art. 65 GDPR dispute resolution procedures aim to resolve disputes between DPAs, rather than to direct the LSA's fact-finding investigations and sanctions.

Relevant information and the right to be heard

> *Given the potential severity of the penalties that may be imposed, parties under investigation for breaches of the GDPR must enjoy guarantees similar to those that are provided for in procedures of a penal character.*[2]

We welcome Art. 8(2)(h) of the proposal, which includes the response of the parties under investigation in the preliminary findings.

For coherence, this response should also be part of the summary of key issues, as described in Arts 9(2)(a) and (b), particularly if corrective measures are envisaged at this stage. Such responses should be reflected in the decision-making process to help provide context to DPAs, ultimately ensuring stronger cooperation.

Where an urgent binding decision is requested from the EDPB, this information could facilitate case resolution by bringing sufficient context. The final text should also ensure that the right to be heard of parties under investigation is respected in urgent binding decisions, with reasonable and proportionate timeframes.

Deadlines for decisions addressed to controllers and processors

Pursuant to Art. 14(4), in preliminary findings, time should be given for the parties under investigation to provide their views. However, the proposal leaves the time limit to the different LSAs to determine. At the very least, the final text should require the deadline to be reasonable and proportionate, and to take into consideration the facts of the investigation. This is necessary to allow the parties under investigation to assess the administrative file they have just received, and provide appropriate responses. Views expressed after the time limit should be considered where they bring new elements to the table, which could affect the final decision.

Similarly, the timeline set by the LSA for parties to make their views known under Art. 17(2), as well as the time limit set by the LSA to raise confidentiality claims under Art. 21(6), should be reasonable and proportionate to the specific nature and complexity of the case.

In the same vein, clear timeframes should be set for LSAs, to foster a harmonised approach and increase clarity and visibility for the parties. We recommend setting a timeframe between 30 and 45 days, depending on the request.

[2] Explanatory Memorandum to the proposal.

The language in Art. 14(6) should be clarified to ensure that the parties' views on the preliminary findings are included in the draft decision. The LSA should not only deal with allegations which parties have been able to provide views upon, but also the actual comments themselves.

Confidentiality of the administrative file

To avoid any misuse of the information parties receive as complainants, careful consideration should be given to confidential information.

Where a non-confidential version of the preliminary findings is shared with the complainant pursuant to Art. 15 of the proposal, information covered by intellectual property rights or trade secrets, or which entails cybersecurity considerations, must remain protected. This also applies when several cases are treated jointly and involve various stakeholders with different interests.

Consideration should also be given to the sensitivity of documents in the administrative file before they are shared. In this regard, we welcome Art. 21(4). However, files should be deemed confidential by default to avoid incorrect assumptions in time-pressing situations. The presumption under Art. 21(7) should therefore be reversed.

Under Art. 21(2), whilst we welcome the exclusion of ongoing files from access requests, the final text should clarify that confidential information remains excluded from the scope of requests after the file closes. Whilst the file might be closed, such information often remains sensitive and confidential.

We also urge that commitments as described in Art. 15(5) should be complemented by sanctions or a specific liability regime for breaches.

Lastly, the right of access to the administrative file, as noted in Art. 19(3), should exclude confidential information when it risks unnecessarily disclosing intellectual property, trade secrets and cybersecurity considerations. To avoid unnecessarily spreading confidential information, where documents prove to be unrelated to the subject matter of the investigation, Art. 19(2) should set an obligation for the LSA to return them. This would also help lower the LSA's costs, resources needed, and efforts in protecting confidential information.

Dispute resolution

We welcome Arts 22-23, which include the views of parties to the proceedings as part of the mandatory list of documents. We recommend that throughout the procedure and investigation, hearings can be presented in oral and written form.

The one-week timeframe under Art. 24(2), and its extension by a week in Art. 24(3), could in some cases prove insufficient to provide an accurate response. Distinctly from the extension available to the EDPB in Art. 24(3), we recommend providing a one-month extension for parties under investigation,

depending on the complexity of the case. This extension would be without prejudice to that foreseen in Art. 24(3).

Annex

The annex presently sets out that a party may include information about the correspondence with the party under investigation in their complaint. In a similar vein, we suggest that information about the company mechanisms used to try and resolve complainants be included here. This would support the investigation and encourage the use of all tools to reach a solution. As detailed above,[3] the annex should include the use of company complaints mechanism in the criteria to assess the admissibility of a complaint.

FOR MORE INFORMATION, PLEASE CONTACT:

Beatrice Ericson
Officer for Privacy and Security Policy
beatrice.ericson@digitaleurope.org / +32 490 44 35

Alberto Di Felice
Director for Infrastructure, Privacy and Security Policy
alberto.difelice@digitaleurope.org / +32 471 99 34 25

[3] See p.3, 'Investigation of complaints.'

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 102 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Applied Materials, Amazon, AMD, Apple, Arçelik, Arm, Assent, Autodesk, Avery Dennison, Banco Santander, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, CaixaBank, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, Honeywell, HP Inc., Huawei, ING, Intel, Johnson & Johnson, Johnson Controls International, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe, NEC, Nemetschek, NetApp, Nintendo, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Pearson, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK