From:	EDPS-NEWS-FOR-DPOS <edps-news-for-dpos@edps.europa.eu>
To:	[redacted]
Sent at:	14/06/21 14:38:24
Subject:	DPS | Quick News for DPOs #20

Dear DPO,

Please find attached the 20th edition of '**Quick News for DPOs**'.

Wishing you a great week ahead!

Yours sincerely,

EDPS S&E Communication Team
| Tel. (+32) 228 31900 | Fax +32(0)22831950 | ›
Email edps@edps.europa.eu
European Data Protection Supervisor
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels
@EU_EDPS www.edps.europa.eu

Quick News for DPOs

May 2021

The EDPS regularly organises training sessions for the staff of European Union institutions, bodies, offices and agencies (EUIs) who deal with personal data in their day-to-day work. These help to ensure compliance with data protection rules and respect for the rights and freedoms of individuals and to encourage the development of a data protection culture within each EUI. These training sessions focus on helping EUIs to go beyond compliance and demonstrate accountability.

1. The use of ICT tools, remote working tools and social media by EUIs

On 17 March 2021, the Supervision & Enforcement Unit (S&E) carried out a two-hour training session for all EUI staff at the European School of Administration (EUSA), focusing on the data protection implications when EUIs use information and communications technology (ICT) tools, remote working tools and social media.

The first hour of the training session focused on the EUIs' obligations when selecting ICT tools for their on-premises or remote work. Based on, but not limited to, the EDPS' Orientations published in July 2020, which address various issues encountered by EUIs as employers, S&E colleagues reiterated that:

- EUI staff should follow their EUIs' established decision-making protocol(s) and involve their data protection officer(s) and IT department(s) when selecting ICT tools;
- EUIs should carefully assess the security, confidentiality and privacy features of the proposed tools and evaluate their potential risks for individuals' personal data, taking into accountant privacy-friendly alternatives that may suit the envisaged purpose of the tool(s). This assessment must also consider whether the tool(s) will be used on corporate and/or private devices; clear policies and instructions for the EUIs' staff must be prepared accordingly so that they can protect themselves and the individuals' personal data that they process;
- the terms of contracts with ICT providers should reinforce EUIs' control over who processes individuals' personal data and how and where this data is processed and provide appropriate safeguards;

- the roles and responsibilities of data processors and sub-processors (ICT/IT providers) should be clearly defined and monitored to minimise risks for the privacy of individuals;
- EUIs should configure the tools so that there is no monitoring of the users by the employer or the provider by default;
- EUIs should configure any new tools with appropriate retention periods in compliance with the purpose of the processing activity and the EUIs' information needs to be deleted or returned after the end of the contract;
- the necessary technical and organisational measures should be put in place to protect individuals' personal data and to respect their rights.

As S&E colleagues moved to the second hour of the training session, they emphasised that the use of social media and videoconference tools should be considered like any other ICT tools when assessing their data protection implications and adopting the necessary measures to insure that individuals' privacy is protected. Like any other processing operation, processing of personal data through such tools used by EUIs has to comply with Regulation 2018/1725.

In addition, when using social media, EUIs should be aware that individuals' data may be processed at different stages and by different actors, this includes:

- users themselves publishing their own personal data;
- users publishing the personal data of others;
- the social media providers establishing users' profiles and analysing information for various purposes;
- third parties receiving information on social media users and combining this with other information that they already have.

These numerous processing operations of personal data increase the risks for individuals and their privacy. Ongoing investigations and court cases - both in EU Member States and at EU level - have sparked questions on the responsibilities of the controller, social media platforms' providers and other actors involved in the processing of individuals' data, whether social media users are sufficiently informed about the way their personal data is processed and, by extension, whether their consent for such processing operations is valid.

EUIs should consider this when they select which social media platform to use, because it has consequences for the individuals, for the EUI and for the EU as a whole. The EDPS intends to test privacy-friendly and open-source alternatives to major social media and videoconferencing tools. In particular, the EDPS intends to test Mastodon and Peertube, alternatives to Twitter and Youtube, as well as the Big Blue Button, alternative to Webex and Zoom.

2. Data protection and online communication

On 25 March 2021, the Technology & Privacy Unit (T&P) presented to the Inter-institutional Online Communication Committee (the IOCC), the EDPS' proposal to pilot Mastodon and Peertube. S&E colleagues also spoke about data protection and online communication, such as social media, to help EUIs navigate this topic.

EUIs, like many other organisations, have increasingly used social media, as well as other online tools, during the COVID-19 pandemic to connect with their audience, such as informing them on their activities or organising webinars.

EUIs need to carefully follow data protection rules when they share personal data, and in particular when they publish them. In particular when using social media platforms, EUIs must consider:

whether the purpose for which they want to process individuals' personal data on social media platforms can be justified under the EU data protection law, Regulation 2018/1725, and in light of the EUIs' tasks;

- what data they can share or publish;
- how to seek consent from individuals whose data may be published, and how to ensure that this data is correct;
- how to delete individuals' personal data if requested once published.

In addition, S&E colleagues also emphasised that it is not because an individual's personal data is public on social media platforms - in the case where the individual has made their pictures or posts on a social media platform public for example - that EUIs can reuse that individual's public information. Data protection rules still apply, meaning EUIs need a legal basis for the processing of that data, they need to inform the individuals about this new processing of their data, set appropriate retention period etc. EUIs should choose the communication and working tools that match a clearly defined use case, including privacy, data protection and security requirements. In line with the principles of data protection by design and by default, EUIs must consider the most data protection and privacy-friendly solutions.

Changing the practices and privacy policies of social media platforms takes a concerted effort. As a member of the European Data Protection Board (EDPB), the EDPS together with the other data protection authorities of the EU issued several guidelines on the application of data protection law and principles when using social media, for example, Guidelines on Social Networking, EDPB Guidelines on the targeting of social media users, as well as many others.

With similarities between the EU data protection law for EUIs, Regulation 2018/1725, and the data protection law applicable to private and public organisations in the EU, the General Data Protection Regulation, these Guidelines aim to help all those who may process personal

data when using social media. For more information, read the EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. The EDPB is also preparing guidelines which will give practical recommendations on data protection in social media platform interfaces.

For more information on past and ongoing cases (in descending chronological order of latest developments) read:

- Norwegian DPA investigation into Facebook (closed)
- Facebook/Cambridge Analytica case of UK DPA (closed)
- Norwegian Consumer Council's report by Deceived by design (closed)
- Dutch DPA investigation into TikTok (ongoing)
- Irish DPA Decision in the matter of Twitter International Company (closed)
- Norwegian DPA: Intention to issue € 10 million fine to Grindr LLC (ongoing)
- Italian DPA imposes limitation on processing on TikTok after the death of a Girl from Palermo (closed, but follow up ongoing in other proceedings)
- Children and Social Networks: Italian DPA Requests Information on Processing from Facebook and Instagram (ongoing)
- Several investigations by Irish DPA concerning Twitter (ongoing) à respect of individual's rights, data security and data breach notification - IE DPA is in particular examining whether Twitter has discharged its GDPR obligations to implement organisational and technical measures to secure and safeguard the personal data of its users (see p. 45 of IE DPA Annual Report 2020).
- La CNIL ouvre une enquête sur l'application Clubhouse (ongoing)
- Wirtschaftsakademie & Fashion ID judgements of the CJEU (closed) à FB Controller Addendum examination by competent DPA(s) is ongoing, however DE DPAs already took the position that Facebook fan pages cannot be operated in compliance with GDPR. The decision will be relevant also for similar services offered by other providers.
- Schrems I & Schrems II v Facebook judgements of the CJEU (closed) à Schrems complaint before Irish DPA and Irish DPA v Facebook case on EU-US data transfers is again ongoing following the judgement of the Irish High Court on procedural matters in relation to inquiry and a preliminary draft decision of the IE DPA against Facebook. The IE DPA will decide if Facebook can lawfully transfers personal data to the US following the Schrems II judgement of the CJEU. The decision will be relevant for similar transfers to the US.
- EDPB taskforce to deal with 101 NOYB complaints on use of Google/Facebook services transferring data to the US is examining these complaints and will decide on the issue of joint controllership and transfers to the US in use of Google Analytics and Facebook Connect services. The decisions will also be relevant for similar services being offered by other providers. Some DPAs have already taken specific positions on transfers in certain online services (e.g. Bavarian DPAs – FAQ – "Internet" or "Internationaler Datenverkher").
- Belgian DPA v Facebook case where BE DPA found non-compliant tracking of users and non-users and invalid consent and issued a ban on Facebook's tracking

of users and non-users in Belgium is à pending before BE courts and before the CJEU and decision will have substantial impact on how Facebook carries out its processing in BE but also throughout the EU/EEA

- Irish DPA statement on Facebook dataset appearing online – IE DPA inquiry into the latest security-related issue involving Facebook is ongoing
- Hamburg DPA urgency measures against WhatsApp - Hamb DPA orders ban of further processing of WhatsApp user data by Facebook

The findings and actions taken by the national DPAs and courts in these cases will affect the very way these platforms work, how the data is processed by the providers and their partners and whether they can still continue with the associated data flows. The road to reaching the end of these cases and the goal of compliance may be long.

The EDPS has not taken a position yet on EUIs' use of major social media platforms and the issues presented in the previous and ongoing cases in EU/EEA Member States. The EDPS however recognises that social networks serving billions of users in all regions of the world are unlikely to deliver in the short term enough reassurance to EUIs that their specific compliance requirements are indeed duly addressed. Until this reassurance is delivered, this means that controllers, EUIs should consider taking other actions in the short and medium term, like looking for alternatives and redesigning their own processing operations, to protect individuals and least of all to be prepared for consequences of enforcement and court decisions.

3. Outsourcing the processing of personal data and procuring products and services

At the request of their data protection officer, the Supervision & Enforcement (S&E) colleagues of the EDPS held two training sessions for Eurojust's members of staff on data protection in procurement and outsourcing of personal data.

The first session, on 19 April 2021, was specifically addressed to Eurojust's management staff, focusing on the responsibilities of the data controller and business units of EUIs to protect individuals' personal data throughout the duration of the contract with an external organisation.

The second session, which took place on 20 April 2021, was for Eurojust's members of staff. S&E colleagues delivered a session on the application of data protection requirements during the different stages of the procurement and outsourcing process: from the call for tender to signing the contract with an external organisation. To ensure that Eurojust's staff is prepared for these procedures, S&E colleagues delivered their training session using several possible scenarios that may occur when managing contracts with external organisations.

Even before commencing the outsourcing of personal data processing or the procurement of products or services, Eurojust's staff - as well as any other EUI - should have a clear plan of

the processing they intend to carry out and the purpose and use that these tools will have, as well as the possible data protection implications and requirements this may entail. Data protection considerations and requirements need to be included already at the stage of the call for tender in procurement documents, where EUIs are describing the elements of the service or product to be provided to them and the conditions under which it is to be provided (EUIs' functional and performance requirements). EUIs need to ask questions and obtain information and guarantees from their processors and providers. Data protection requirements then have be included in the contract and any other documents, instructions and non-contractual (technical and organisational) measures agreed with the processor or provider. This will allow Eurojust to ensure a tailor-made contract during which they will have full control over how, when, why, where, what type of personal data is processed and by whom. EUIs must only use processors providing sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of Regulation 2018/1725, as well as any other applicable EU law (e.g. Eurojust Regulation), and ensure the protection of the rights of individuals. In this sense, Eurojust, or the EUI in question, should ensure clear documentation of the products and services it uses and the processing done on its behalf, evidence that these tools and processing operations will - and must - incorporate the privacy by design and privacy by default principles.

When contracting products and services from an external organisation that may involve the processing of personal data in a non-EU country, EUIs must ensure that the protection afforded to the transferred personal data in that country is essentially equivalent to that guaranteed in the EU. If any supplementary measures are needed to ensure the required level, EUIs must implement them, where necessary together with the data importer.

The EUIs need to periodically re-evaluate their processing operations, their tools, and their data protection safeguards and measures - this also includes data protection safeguards and measures in their contracts with external organisations - and readjusting these if necessary.

The EDPS advises EUIs in developments of inter-institutional public procurement, on arrangements with processors, on arrangements with joint controllers and on transfers to third countries and international organisations. For more information, read:

- EDPS Public paper on the outcome of its own-initiative investigation into the use of Microsoft products by EUIs (2020)
- EDPS Guidelines on concepts of controller, processor and joint controllership (2019)
- EDPS Guidelines on IT governance and IT management (2018)
- EDPS Cloud Computing Guidelines (2018)
- EDPB Guidelines on Data Protection by Design and by Default (2019/20)
- EDPB Guidelines on concepts of controller and processor under the GDPR (2020) (update of WP29 Opinion 1/2010 (WP169))
- EDPB Recommendations 01/2020 on supplementary measures (2020) - These Recommendations adopted last November are currently being reviewed following the public consultation, however the Recommendations became applicable immediately following their publication.

4. What should data exporters (like EUIs) think about when transferring data from the EU following the Schrems II judgement of the CJEU?

This is precisely the question that the EDPB recommendations 01/2020 on supplementary measures tried to address. These Recommendations adopted last November are currently being reviewed following the public consultation, however the Recommendations became applicable immediately following their publication. As for now and in a nutshell, there are several steps that EUIs should take before transferring their personal data:

Step 1 - know your transfers

What does it mean?

- To be aware of all transfers i.e. to map all the transfers.
- To take into account onward transfers (to other recipients within the same third country or to other third countries).
- To have the full picture before starting the transfer.
- In line with existing obligations in Articles 4, 5, 6, 26, 29, 30 and Chapter V of the Regulation, the EUIs need to know and control data flows. So, any data flows within or outside the EEA, onward transfers and use of a sub-processor can only happen if you (EUIs) as the controller have allowed it.
- Keep in mind that remote access from a third country (for example in support situations) and/or storage in a cloud situated outside the EEA offered by a service provider, is also considered to be a transfer.

Step 2 – identify the transfer tools you are relying on

- Adequacy decisions: no need for supplementary measures, provided you and data importer have implemented measures to comply with the other obligations under the GDPR/EUDPR; otherwise implement those measures.
- Article 46 GDPR / 48 EUDPR transfer tools: candidates for supplementary measures depending on the third country law/practices.
- Derogations Article 49 GDPR / 50 EUDPR: no need for supplementary measure.

Step 3 – assess whether the transfer tool is effective (the key step)

The transfer tool must ensure that data subjects are afforded a level of protection in the third country that is essentially equivalent to that guaranteed within the EU.

How to do that?

- Assess whether there are problematic laws in force in the country to which data is transferred (or onward transferred) that affect your specific transfer, i.e. laws that impinge on the effectiveness of the transfer tool you are relying on.
- In case there are no laws identified, there will still be a need to look for other relevant and objective factors that affect your specific transfer, i.e. unlawful practices.
- The scope of your assessment is limited to the legislation and practices relevant to the protection of the specific data you transfer. So this is not the general and wide encompassing adequacy assessment that the Commission carries out in accordance with Article 45 GDPR.

Outcome of the assessment:

- The transfer tool can be effectively applied (e.g. because no inadequate law or the inadequate law does not apply to the transfer at hand): no need for supplementary measures. or
- The transfer tool cannot be effectively applied: need for supplementary measures or else no transfer can take place.

Step 4 - identify and adopt supplementary measures

- This is a case-by-case analysis.
- Different types of supplementary measures: of a technical, contractual and organisational nature.
- Annex 2 of the EDPB Recommendations 01/2020 gives examples of supplementary measures. For each measure to be considered effective, a series of conditions have to be complied with.
- Contractual and organisational measures alone will generally not overcome unlawful access by public authorities of the third country.
- In case effective supplementary measures can be identified: transfer can take place.
- In case effective supplementary measures cannot be identified: no transfer and if it already took place: suspension or end of the transfer. If the data exporter decides to nevertheless transfer the data: notification to the SA which will suspend the transfer in case it finds that the level of protection is not essentially equivalent (and may take any other corrective measures).

Step 5: procedural steps after having identified the supplementary measures

- SCCs: no need to request an authorisation from the SA.
- BCRs and ad-hoc contractual clauses: Schrems II also applies. Precise impact is still under the discussion and may be detailed in other documents (e.g. BCRs referentials).

Step 6: re-evaluate at regular intervals

Why? Because accountability is a continuous obligation.

Need to put mechanisms in place to ensure prompt suspension or end of transfers where:

- the importer has breached or is unable to honour the commitments it has taken in the Article 46 GDPR / 48 EUDPR transfer tool; or
- the supplementary measures are no longer effective in that third country.

For more information:

- The FR Council of State asks the Health Data Hub for additional guarantees to limit the risk of transfer to the US
- FR Council of State - The urgent applications judge does not suspend the partnership between the Ministry of Health and Doctolib for the management of COVID-19 vaccination appointments
- Bavarian DPA (BayLDA) calls for German company to cease the use of 'Mailchimp' tool
- Census 2021: Portuguese DPA (CNPD) suspended data flows to the USA
- EDPS Opinion on Online Event Management at EACEA (Case 2020-1119)

On 22 June 2021, S&E colleagues will continue their thematic trainings for EUI staff organised by EUSA dedicated to international transfers, which will look more in detail at the conditions and safeguards for such transfers. Interested EUI staff can enrol in EU Learn. Should your EUI staff not have access to EU Learn, please inform us about expressed

5. Have a great day!

Feel free to share this newsletter with your DPCs!

For more information on how the EDPS collects your personal data, see our data protection notice.