ELVINGER HOSS PRUSSEN

ELVINGER HOSS LUXEMBOURG LAW

ICT, IP, media and data protection NEWS

TABLE OF CONTENTS

EDPB Statement about transfers of personal data to Russia

What happened?

On 12 July 2022, the European Data Protection Board (the "**EDPB**") published a Statement 02/2022 on personal data transfers to the Russian Federation. As a consequence of the war initiated by the Russian Federation against Ukraine, Russia has been excluded from the Council of Europe and is therefore no longer a contracting party to its respective conventions and protocols. Russia will also cease to be a contracting party to the European Convention on Human Rights as of 16 September 2022. According to the EDPB, these changes will have a significant impact on the level of protection of data subjects with respect to the transfers of personal data from the European Economic Area (the "**EEA**") to Russia.

In their statement, the EDPB does not comment on the lawfulness or unlawfulness of such transfers. The EDPB rather concludes that frequent exchanges of personal data still exist due to "close economic and historic ties" and that supervisory authorities continue to monitor legislative changes and other relevant developments in Russia that may have an impact on data transfers.

What are the next steps?

Following the Schrems II ruling and the successive recommendations of the EDPB, data exporters are responsible for assessing whether, in the context of a transfer of personal data, the applicable legislation in the destination jurisdiction is likely to undermine the effectiveness of the appropriate safeguards of the instruments of Chapter V GDPR:

- if this is the case, exporters should identify and adopt the additional measures that are necessary to ensure a level of protection for data subjects that is substantially equivalent to that guaranteed within the EEA;
- if this is not the case and no additional measures can be identified, data exporters should suspend the data transfers.

This may also interest you:

- **CJEU invalidates the Privacy Shield: implications for EU-US personal data transfers**
- **EDPB Recommendations 01/2020 and 02/2020 on transfers of personal data after Schrems II**

For any questions, please contact

View profile

Gary Cywie

Partner

The New Copyright Directive finally transposed into Luxembourg law!

What happened?

On 1st April 2022, Luxembourg enacted the **law** [1] aiming at transposing into Luxembourg law the *Directive 2019/790 on copyright and related rights in the Digital Single Market*("New Copyright Directive") adopted on 17 April 2019[2].

This new law modifies the three following laws:

- the Law of 18 April 2001 on authors' rights, related rights and databases, as amended,
- the Law of 3 December 2015 on certain authorised uses of orphan works, and
- the Law of 25 April 2018 on the collective management of author's rights and neighbouring rights.

What are the key takeaways?

The Luxembourg law faithfully transposes into Luxembourg law the New Copyright Directive, which aims at modernising the legal regime of authors' rights and neighbouring rights. The purpose of the New Copyright Directive was to take into account the major technological developments of the last twenty years and the new ways of creating, producing, distributing and exploiting works and other protected content.

The main changes to the authors' rights regime are the following:

- The creation of neighbouring rights for press publishers (the right of reproduction and the right of making press publications available to the public) in relation to the use of their content online; subject to certain limitations, this would allow press publishers to ask for remuneration when their content is reused by online platforms, news search engines and news aggregators.
- The creation of an authorisation mechanism and a new liability regime regarding specific uses of protected content by online content-sharing service providers (such as YouTube).
- the creation of new exceptions to the authors' rights to promote, in particular, text and data mining under certain conditions (which is a set of automated techniques aiming at analysing texts and data in digital form in order to extract information) and the digital use of the works, exclusively for purposes of illustration in the context of teaching, to the extent justified by the non-commercial purpose pursued;
- the enshrinement of a principle of appropriate and proportionate remuneration for authors when they conclude licence agreements or assignment agreements about the exploitation of their work, as well as a possibility for authors to ask for an additional compensation. The parties with whom the authors have signed a licence or an assignment agreement must provide the authors, at least once a year, with information on the exploitation of their works in particular with regard to the total income generated. If the remuneration initially agreed upon proves to be unreasonably low in comparison with the total income derived from the exploitation of the works, then the authors will have the right to an appropriate and fair additional remuneration.

Conclusion

It remains to be seen whether the new law will entail more balanced relationships between the various players of the Luxembourg market regarding the use and exploitation of works and protected content.

The new law will come into force on 9 April 2022

For more information about the New Copyright Directive, please see our previous articles on this topic:

- **Adoption of new European Copyright Directive**
- **Transposing New Copyright Directive – Luxembourg draft legislation**
- **Bill of Law 7847 transposing New Copyright Directive**

> 1. Resulting from Bill of Law 7847.
> 2. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

For any questions, please contact

View profile

Emmanuèle de Dampierre

Counsel

Proposed EU Data Act open for feedback from stakeholders until 11 May 2022

Why a Data Act?

On 23 February 2022, the European Commission adopted a **Proposal for a Regulation on harmonised rules on fair access to and use of data** (the **Data Act**) as part of its set of measures related to the **European Data Strategy**.

An explanatory memorandum accompanies the Data Act detailing the reasons for and objectives of the proposal. As a key pillar of the European Data Strategy, this act aims at contributing to the creation of a cross-sectoral governance for data access.

The European Commission is hence willing to foster access to and use of data between various players, notably by way of protecting small and medium-sized enterprises (**SMEs**).

What's in the Data Act?

The proposed Data Act pursues several objectives propelling a virtuous circle of data sharing between consumers and private and public entities. In particular, it aims at:

- facilitating access to and use of data by consumers while preserving incentives to invest in ways of generating value through data; this means that, by default, users must be able to easily, securely and "where relevant and appropriate", directly access data generated by their use of a product or service;
- providing for the use by public sector bodies and EU institutions, agencies, or bodies, of data held by enterprises in certain situations where there is an exceptional data need (i.e. in cases where compulsory business-to-government data sharing is justified);
- facilitating switching between cloud and edge services;
- putting in place safeguards against unlawful data transfers;[1]
- ensuring that data holders avoid unilaterally imposing unfair contractual terms to SMEs.

The Data Act would also slightly modernise certain concepts linked to the *sui generis* right protecting databases by intellectual property rights.

Interactions between the Data Act and other EU laws

The proposed Data Act relies on a broad definition of the concept of "data" which include both personal and non-personal data. The proposed Data Act would apply without prejudice to the EU General Data Protection Regulation 2016/679 (the **GDPR**). In that respect, the proposed Data Act recalls that the use of a product or service may, particularly when the user is a natural person, generate data that relates to an identified or identifiable natural person (the data subject). In such circumstances, the processing of that data remains subject to the rules set out under the GDPR including "where personal and non-personal data in a data set are inextricably linked."

As indicated above, the proposed Data Act shall be read in the light of the European Data Strategy. The proposal complements and shall be read in conjunction with (i) the proposed Data Governance Act (**DGA**) which notably harmonises conditions for the use of certain public sector data and (ii) the proposed Digital Markets Act (**DMA**) requiring providers of "core platform services" identified as "gatekeepers" to provide certain portability features to the benefit of business and end-users.

Please see our other publications about the **DMA** and the **DGA**.

Next steps

The feedback from stakeholders (that can be provided **online** will be presented to the European Parliament and Council for consideration during the legislative debate.

1. Chapter VII of the Data Act specifically relates to the prevention of unlawful access to or disclosure of non-

> personal data held in the European Union. Such developments are in fact quite similar to the provisions set out under Chapter V of the GDPR regulating the lawful disclosure of personal data to third countries.

For any questions, please contact

View profile

Gary Cywie

Partner

Focus on European Commission's proposal for a Digital Services Act

On 15 December 2020, the European Commission published the Digital Services Act Package, which includes two significant proposals:

- a **proposal for a Regulation on a Single Market For Digital Services** (Digital Services Act or "**DSA**") and amending Directive 2000/31/EC ("**e-Commerce Directive**"),
- a proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Act or "**DMA**").

These proposals are expected to affect various types of providers of digital services (such as marketplaces, social media platforms, content-sharing platforms) in the European Union ("**EU**") and to create a safer and more open digital space while further developing the European Single Market for digital services.

The proposal for a Digital Services Act ("**DSA Proposal**") clarifies and upgrades the responsibilities and the accountability of the digital service providers with respect to any illegal content they intermediate or disseminate without wiping out past principles. The DSA Proposal sets out several layers of obligations, which shall apply to the digital service providers depending on the type of services they provide in the digital space.

For more information with respect to the DSA Proposal (context, entities targeted, key obligations, supervisory framework, sanctions), please read our article **here**.

As for the DMA, it will impose obligations for large online platforms (*e.g.* online search engines, video-sharing platform services, cloud computing services) that behave as "gatekeepers", such status being more fully defined in the DMA. The DMA aims to refrain from anti-competitive and unfair practices and ensure that gatekeepers themselves act in a way that guarantees an open online environment.

Calculation of fines under the GDPR: draft guidelines by and for the authorities

On 12 May 2022, the European Data Protection Board (the "**EDPB**") published its Guidelines 04/2022 on the calculation of administrative fines (the "**Draft Guidelines**") under Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (the "**GDPR**"). The Draft Guidelines provide for a harmonised calculation of administrative fines under the GDPR. In general, the calculation of administrative fines is at the discretion of national data protection authorities ("**DPAs**"), which must assure that the latter remain effective, proportionate and dissuasive in each individual case. Under the Draft Guidelines, the EDPB provides for a *five-step methodology* which DPAs should apply when calculating administrative fines.

Step 1: Determining whether there are one or multiple infringements against the GDPR

First, DPAs should consider the conduct and the GDPR infringement of the controller or processor. Depending on the case, DPAs may identify either one or multiple sanctionable conduct according to which the scope of the administrative fine will differ:

- if there is only one sanctionable conduct, DPAs should establish whether or not the alleged conduct gives rise to one or more infringements and whether those infringements are to be considered individually or alongside each other;
- if multiple sanctionable conducts are identified (e.g. different processing operations infringing different requirements stemming from the GDPR), the undertaking can be subject to separate fines applicable for each infringement of the GDPR (in which case the maximum monetary cap for a fine in relation to the same or linked processing operations shall not apply).

As a result, in practice, the aggregate amount of fines may exceed the absolute maximum of 4% of the annual worldwide turnover of the undertaking or EUR 20,000,000, whichever is higher. Also, it is confirmed that the concept of "undertaking" includes group companies.

Step 2: Setting out the starting amount of the fine

To determine the adequate starting amount to consider for the further calculation of the administrative fine, the Draft Guidelines provide that DPAs shall notably assess the degree of seriousness of the infringement by giving due regard to the nature, the duration and the gravity of the infringement and finally take into account the turnover of the undertaking acting as controller or processor.

Step 3: Evaluation of aggravating and mitigating circumstances related to past or present behaviours

Next, DPAs shall determine whether there are any aggravating or mitigating circumstances, in the past or present, against the data controller or processor, that could justify increasing or decreasing the amount of the fine. In particular, DPAs should, in the event of an infringement, focus on the actions taken by the controller or processor to mitigate the damage suffered by the data subjects.
In this regard, it is specified that cooperation with the authorities is a general obligation under the GDPR and should not be taken into consideration for the determination of the amount of the fine, except if

such cooperation results in mitigating risks for the individuals affected by the infringement at stake.

Step 4: Identification of the relevant legal maximums for the alleged processing operation

As a fourth step, the DPA should identify the maximal legal amount for the processing operation at stake as provided by Articles 84(4)-(6), namely either:

- a fine of maximum EUR 10,000,000 or 2% of the undertaking's annual worldwide turnover, whichever is higher or,
- a fine of maximum EUR 20,000,000 or 4% of the undertaking's annual worldwide turnover, whichever is higher.

Step 5: Analysis of whether the calculated fine meets the requirement of effectiveness, dissuasiveness and proportionality

Finally, the DPA shall assess whether the final fine meets the requirements of effectiveness, dissuasiveness and proportionality as required by Article 83(1) of the GDPR.

With respect to its proposed methodology, the EDPB emphasises the fact that the calculation of an administrative fine is not a mathematical exercise, but rather a process which must take into account the specific circumstances of each case.

What's next?

The Draft Guidelines are subject to public consultation and open for comments. Stakeholders can submit their feedback until 27 June 2022 after which the EDPB is expected to adopt its final guidelines.

For any questions, please contact

View profile

Gary Cywie

Partner

GDPR: EU Commission's Q&A about the New Standard Contractual Clauses for Transfers

What happened?

On 25 May 2022, exactly 4 years after entry into force of the General Data Protection Regulation ("**GDPR**"), the European Commission (the "**Commission**") released new guidance on Standard Contractual Clauses (the "**SCCs**"). Earlier in 2021, the Commission adopted a **new set of SCCs** aiming at providing greater flexibility for cross-border data transfer of personal data from the European Economic Area to third countries not benefiting from an adequacy decision. The Commission published **Questions and Answers** on SCCs based on feedback received from various stakeholders and addressing 44 practical questions raised about the new modular-type SCCs (the "**Q&A**").

What are the key takeaways?

- The Q&A confirms that the text of the SCCs may not be altered except (1) to select modules or specific options offered in the text, (2) to complete the text where necessary (3) to fill in the Annexes or (4) to add additional safeguards. None of these actions are considered as altering the core text.
- However, the parties may supplement the SCCs with additional clauses or incorporate them into a broader commercial contract, as long as the other contractual provisions do not contradict the SCCs, either directly or indirectly, or prejudice the rights of data subjects.
- The Q&A also provides practical guidance with respect to the "docking clause" which is an optional clause allowing an additional party to join a contract. All the pre-existing parties may provide consent. The formalisation of such consent is governed by national law and not by the SCCs. In order to make the accession of the contract effective, the new party will need to complete the Annexes and sign Annex I of the SCCs. Upon accession to the SCCs the party will assume all the rights and obligations according to its role and the other parties will simultaneously have the relevant rights and obligations vis-à-vis the new party.
- SCCs can be signed electronically if the national law governing the agreement allows conventions to be signed electronically.
- The Commission also confirmed that processors are required to provide the names of their respective sub-processors. It is not sufficient for the processors to provide only the categories for the sub-processor.
- Finally, the Q&A provides important guidance on the four different modules to the SCCs, the contexts in which they are to be used as well as how the new SCCs are to be used in a post Schrems II[1] context (read more about the Schrems II case **here**).

Next steps

Transfer of personal data outside of the EEA to countries not benefiting from an adequacy decision can only be made if the data exporter –i.e. you or the (sub-)processor, as applicable– provide appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

SCCS may, depending on the circumstances, provide such appropriate safeguards. Hence, if you or any of your (sub-)processors processing personal data on your behalf or, in turn, on behalf of your own processors transfer or intend to transfer personal data as mentioned above, SCCs might be the right

choice. SCCs might need to be supplemented by specific measures according to the situation at hand.

We can provide you with any advice in this respect. We have developed an internal tool to quickly and efficiently provide you with the SCCs modules or any of them alone that your transfers require!

1. Case C-311/18, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems.

For any questions, please contact

View profile

Gary Cywie

Partner

Digital Market Act, Digital Services Act,Data Governance Act and Data Act: quick guide to EU regulations on digital and data strategy!

From November 2020, the European Commission proposed a set of four regulations aiming at the implementation of EU's digital and data strategy: the **Digital Market Act**, the **Digital Services Act**, the **Data Governance Act** and the **Data Act**.

In this digital leaflet, we propose a quick guide to these EU regulations by providing briefly for each of them its purpose, to whom it is addressed, the main takeaway, a status on the adoption process and its (expected) entry into force.

For any further information please contact us or visit our website at **www.elvingerhoss.lu**.

The information contained herein is not intended to be a comprehensive study or to provide legal advice and should not be treated as a substitute for specific legal advice concerning particular situations.

We undertake no responsibility to notify any change in law or practice after the date of this newsletter.