Rådet for Digital Sikkerhed

21 December 2021

Conflict in requirements for data controllers between Article 32 and Chapter V

The Danish Council for Digital Security (Rådet for Digital Sikkerhed (RfDS)) is of the opinion that the requirements for the protection of data subjects in Article 32 of the GDPR and the requirements for third-country transfers in Recommendation 01/2020, in the light of the Schrems II verdict's interpretation of Chapter V of the GDPR, are in some cases incompatible in practice. This means that there is a conflict of provisions and that data controllers cannot in practice fulfil both obligations at the same time. If controllers refrain from implementing necessary risk based Article 32 measures to comply with Recommendation 01/2020 this will be to the detriment of the data subjects.

Therefore, RfDS recommends that the EDPB allows data controllers to conduct a proportionality assessment in favour of Article 32 and at the expense of Chapter V in cases where technical measures are not available to fulfil both obligations. If the EDPB does not consider that a proportionality assessment can be made, the EDPB is asked to recommend alternative solutions to resolve the conflict of provisions.

Background

RfDS has for many years followed the development of regulation in the field of personal data law, including the development of regulation in relation to third-country transfers. RfDS is of the opinion that the EDPB's Recommendation 01/2020 makes it impossible in practice for data controllers to provide protection corresponding to the risk for data subjects.

Recommendation 01/2020 recommends 1) a six-step transfer impact assessment, 2) identifies three possible outcomes for transfers to countries with problematic legislation in Section 43, 3) states in Section 53 that organisational and contractual measures are not sufficient, and that the data controller must rely on technical measures and finally 4) in case 6 states that personal data must not be available in clear text when a third country transfer takes place.

Furthermore, when processing personal information data controllers must implement measures to ensure a level of security appropriate to the risks for the rights and freedoms of data subjects under Article 32.

Data controllers are thus faced with requirements for measures to ensure an essentially equivalent level of protection when transferring personal data to third countries and requirements for measures to provide a level of security appropriate to the risks of data subjects when procession personal information in general.

The challenge

Article 32 requires data controllers to carry out a risk assessment and to choose for each risk an appropriate Article 32 measure corresponding to the risk. In practice, the data controller draws up a requirements specification that ensures that the Article 32 measure can fit into the existing IT-operations environment while appropriately reducing the risk to the data subject. Possible suppliers who are deemed to be able to meet the requirements are then invited to present their security measures. As part of meeting all the requirements, a TIA is also made assessing the transfer tool.

In practice, it turns out that many Article 32 measures either originate from US suppliers or involve US suppliers because part of the functionality or hosting of the solution lies with a US cloud provider in a European data centre. Few security vendors are of European origin, and most of these, as mentioned, use US functionality.

The Danish Council for Digital Security
Vester Farimagsgade 37B, 1. th., 1606 Copenhagen V
Telephone: +45 53 36 02 23 email: info@digitalsikkerhed.dk web: www.digitalsikkerhed.dk

Thus, in the data processor agreements available from the Article 32 suppliers, it is most often stipulated that there will be access to data from supporters in third countries with an aim of solving technical problems, from technical specialists who monitor threats in managed solutions 24/7/365, from affiliate companies in the data processor's group in third countries, from sub-data processors in third countries or by from law enforcement authorities in the third countries by injunction against the data processor's parent company.

A few cases can illustrate the issue.

DDoS measures

Distributed Denial of Service (DDoS) attacks are cyber-attacks that aim to overload a legitimate service or network with a lot of illegitimate traffic so that the service or network becomes inaccessible to legitimate traffic and thus stops working. In order to ensure availability to the data subject, many risk assessments will require implementing an anti-DDoS solution.

DDoS attacks can occur at different layers of the OSI model, but a classic attack is a SYN flooding attack. In such an attack, the attacker exploits the fact that when establishing a connection between, for example, a web client and a web server, three packets are usually exchanged: clients send a SYN packet to synchronise, the server replies with a SYN-ACK packet to signal that it will accept the synchronisation, and the client replies with an ACK packet confirming the connection. If the client does not send the last ACK packet, the server will be on a half-open connection waiting for the ACK packet. When there are enough half-open connections, the server cannot handle any more of them, and then the server crashes because it does not respond to legitimate traffic.

In order to protect against this type of attack on a large scale, it is necessary to route all traffic through a third party, which analyses the traffic and removes the part deemed to be malicious (scrubbing). For example, cloud-based proxies can be used to create filters that remove certain types of traffic based on historical attack vectors (CDN protection). When deciding which traffic to remove, data such as IP address, host name, geolocation, and other online identifiers and most of this data will be personal data.

Protecting against DDoS typically requires access to a very large infrastructure that can handle huge amounts of data. In practice, the largest providers in this segment of the security market are US companies and/or data processing often ends up in the largest data centre providers, which are American. This type of measure would therefore conflict with the recommendations of Recommendation 01/2020 because the controller cannot ensure an adequate level of protection.

EDR measures

Ransomware is malicious software that encrypts any data the software can get its hands on, with the aim of extorting money from the victim. Ransomware is probably the biggest threat to European data controllers. In order to protect against ransomware and other advanced threats, you need to move beyond old-fashioned signature-based protection and have tools that support anomaly-based protection, i.e. automatic pattern recognition of malicious software behaviour. The disadvantage of signature-based protection is that it can only catch the maliciousness that is known, whereas anomaly protection has the ability to detect unknown threats in the infrastructure.

Endpoint Detection and Response (EDR) is one of the technologies that can be used to protect against ransomware and other advanced threats. An EDR platform requires that each machine (endpoint) in the network is actively monitored by a running EDR process, which can automatically detect and react in case of suspicious behaviour in a process on the machine. In order to function, EDR collects a large amount of telemetry on endpoints, including data on running processes, network connections, service creation, user logins, IP addresses and other identifiers. Part of this telemetry is personal data. All that telemetry data is indispensable for detecting threats and impossible for an ordinary human or even a SOC function to analyse manually, which is why one uses anomaly-based protection. Using machine learning models for anomaly detection that run on top of telemetry data, it becomes possible to detect unknown threats in the infrastructure and isolate or stop the threat.

Telemetry data, static signatures and various machine learning models are often processed by the service provider in a cloud data centre and possibly shared (in partially anonymised form) across EDR customers around different countries to provide better protection and the ability to block threats as they arise. Without this sharing, the protection of data subjects will be severely impaired.

In practice, some of the largest providers in this segment of the security market are US companies and/or data processing from European service providers often ends up in the largest data centre providers, which are American. This type of measure would therefore conflict with the recommendations of Recommendation 01/2020 because the controller cannot ensure an adequate level of protection.

Anti-phishing

Phishing is a social engineering attack that uses charm, trickery, or threats to lure users into clicking on a malicious link that can be used to spread ransomware, steal identities, credit card details and more. Phishing is the most common method of spreading ransomware. Also, in anti-phishing solutions, a lot of telemetry data is collected about the sender, recipient, subject, links, IP address of sender and recipient, and other data from the mail header, which is covered by the concept of personal data. Machine learning models are also used for anomaly detection in order to also find the unknown threats that are not caught by the signature-based rules on the basis of e.g. blacklists (IP addresses, domains, hashes), etc.

As with EDR, this personal data is typically processed by the service provider in a cloud data centre and may be shared with customers in a partially anonymised form.

In this area, there are US and European services as well as services from approved third countries, but the services, in turn, end up in a US-based European cloud data centre. Once again the Article 32 security measure would therefore conflict with the recommendations of Recommendation 01/2020 because the controller cannot ensure an adequate level of protection.

Other conditions

In addition to the purely technical issues discussed in the cases above, which make it impossible to comply with both Article 32 and Chapter V at the same time, the overall assessment is that it is very opaque what data ends up where. Most service providers claim to be GDPR compliant, and it requires significant technical and legal skills that few companies possess or have access to in order to determine whether a provider is compliant or not. Moreover, the skills needed to conduct these assessments are very scarce and expensive, hampering the ability of many smaller data controllers to conduct a compliance assessment.

As the cases above illustrate, complying with Chapter V in the interpretation of Recommendation 01/2020 it will be impossible to implement appropriate Article 32 measures in many areas because most of these will end up in the cloud not offering an essential equivalent level of protection.

The consequence is eighter that Article 32 measures are chosen, which basically do not provide an essentially equivalent level of protection, or necessary Article 32 measures are opted out, thus putting data subjects at risk when personal data are processed. In a number of cases, the data controller may not be able to be compliant with both requirements.

The threat landscape

The threat landscape is changing constantly and rapidly. All natural persons have data that is of value to cybercriminals. All legal entities have data on natural persons that are of value to cyber criminals. Cyber criminals have powerful resources at their disposal. They combine their professional skills in informal networks across the globe to create malicious code, or they are sponsored by a state actor for whom they conduct their cybercrime. Threats to data are in the latest top five in the ENISA Threat Landscape along with ransomware and malware, among other things. Where cybercriminals cannot directly target a victim, they attack the value chain and find the weakest link to gain access.

With the evolving threat landscape, it would be to the detriment of both organisations and data subjects if data controllers are to refrain from providing risk based necessary Article 32 measures for the sake of Chapter V.

Nature of Article 32 measures

Article 32 measures differ from other processing of personal data in that the GDPR requires their implementation – this does not apply to e.g. ERP, CRM, HR, email, and telephony systems. The processing of personal data that takes place as a result of Article 32 measures thus cuts across other systems and processing operations precisely to ensure that no threat to the data subject arises from these other processing operations. **Processing of personal data in Article 32 measures, therefore, has a different nature from the other processing operations.** To some extent, this also seems to be recognised in the GDPR, in that recital 49 provides a reasonable framework for implementing Article 32 measures based on legitimate interests.

Article 8(1) of the Charter reads: 'Everyone has the right to the protection of personal data concerning him or her'. In both Schrems I and II, the Court of Justice of the European Union (CJEU) has placed great emphasis on the protection of data subjects contained in the Charter when processing personal data. Thus, in Schrems II, the CJEU was assessing the law in place to protect data subjects when processing personal data in the US and the practice of surveillance of data subjects, including mass surveillance, as revealed by Snowden. The CJEU found that the surveillance was not proportionate to what could be expected in a democratic society, and thus that the transfer to the US did not provide an essentially equivalent level of protection of the data subjects' rights (there were other grounds, including a judicial review under Article 47 of the Charter, but we will not go into that here). Thus, personal data is not properly protected when transferred to the US.

The processing operations under Article 32 also help to provide the "protection of personal data relating to" the data subject, cf. Article 8 of the Charter. **Processing under Article 32, therefore, support the data subject's rights in the Charter at least as much as processing under Chapter V.** Therefore, processing

according to Chapter 32 has its own nature, which is different from ordinary processing in, e.g., an ERP, CRM, HR, email, and telephony system.

In addition to Article 8 of the Charter, EU citizens are also given other rights. They are given the right to do business in Article 16, the right to good administration in Article 41 and a host of other rights. For many of these rights, it is a prerequisite that personal data can be processed – and that these are processed securely. **Both Chapter V and Article 32 of the GDPR thus support the rights of the Charter together, and not only Article 8 of the Charter. However, when it is not possible in practice to fulfil both obligations simultaneously, it must be determined that a conflict of provisions exists.** Therefore, when one has to be able to exercise one's right to the protection of personal data at the same time as one can exercise the other rights, it seems relevant to allow a certain proportionality in the assessment of the measures that ensure the exercise of the rights. In concrete terms, it seems reasonable to allow an assessment of the proportionality between the Chapter V measures and the Article 32 measures, rather than simply dogmatically requiring that both be fulfilled at the same time when the consequence is that processing must cease because measures cannot be found that provide compliance with both Article 32 and Chapter V at the same time. This would be to the detriment of the administration, businesses, and citizens alike. **As a result, RfDS is of the opinion that the data controller should be allowed some proportionality assessment of the use of measures according to Article 32 even if these do not comply with the requirements of Chapter V.** More concretely, we envisage that the data controller may consider that a given Article 32 measure is so important for the protection of the rights of the data subject that compliance with Chapter V can be compromised.

In this context, it is worth mentioning that recital 4 of the GDPR precisely states that **the right to data protection must be 'balanced against other fundamental rights, in accordance with the principle of proportionality'.** It should also be mentioned that the CJEU in the Schrems II judgment presumably does not provide for *the same level of protection* but an *essentially equivalent level of protection*, and thus it must be possible to conduct a proportionality assessment of measures protecting the overall rights in the Charter. Furthermore, in the Schrems II case, the Court of Justice of the European Union seems to have considered only the circumstances of transfers and not the relationship and the conflict of provisions between Article 32 and Chapter V. Finally, both Article 5 of the EU Treaty and Article 52 of the Charter provide for a proportionality point of view to be applied in the exercise of the rules.

Narrow scope

RfDS notes, that **the proportionality assessment that RfDS considers there is room for has a narrow scope**. It can only apply to processing of personal data in risk-based Article 32 security measures required by the GDPR – and thus not in relation to all other possible processing activities (e.g., processing in ERP, CRM, and other systems in the cloud). Proportionality assessments can also only take place for measures where there is a conflict of rules between Article 32 and Chapter V, which means that the rights in the Charter cannot be fulfilled – and thus not for all Article 32 measures where one could easily find measures that comply with both Article 32 and Chapter V. Thus, the proportionality assessment will certainly be more important in the present than in the future where measures that will be compliant with both Article 32 and Chapter V must be expected to be innovated in the European market. However, in the long term, it will still be necessary to have the possibility to make the proportionality assessment – for example, in the scenario where a new significant threat to data subjects arises, and a new Article 32 measure is first developed in a third country.

Rådet for Digital Sikkerhed

21 December 2021

Summary and solution

As mentioned above, in many cases, it is not possible for data controllers to be compliant with both Article 32 and Recommendation 01/2020 at the same time. At the same time, the threat landscape evolves continuously and with significant speed, to the detriment of data subjects if not mitigated with appropriate measures.

Furthermore, within the scope of the General Data Protection Regulation and the Charter for processing operations related to security measures, there seems to be room to apply a proportionality point of view in favour of Article 32 and at the expense of Chapter V in those situations where alternative measures cannot reasonably be found that meet both requirements.

With this letter, RfDS wishes to draw the attention of the EDPB to the conflict between Article 32 and Recommendation 01/2020.

RfDS kindly requests the EDPB to consider whether a proportionality assessment can be made between Article 32 and Chapter V in cases where both obligations cannot be fulfilled simultaneously.

If the EDPB does not find that a proportionality assessment can be made, the RfDS will kindly requests the EDPB to recommend alternative solutions where there is no risk based necessary Article 32 measures that are compliant with Recommendation 01/2020.

The Council is, of course, available to elaborate on the above views.

On behalf of the Board

Henning Mortensen
Chairman, Danish Council for Digital Security

About the Danish Council for Digital Security (RfDS)

RfDS is a Danish private NGO promoting a safe and free digital society for all. RfDS is independent and receives no public funding. Member organisations include public authorities, municipalities, universities, employers' associations, trade unions, consumer organisations, rights organisations, and private companies of both a national and global nature.

RfDS has been very involved in the Danish debate on personal data protection for many years. RfDS has thus published many guides and awareness materials to promote knowledge of and to operationalise the personal data regulation.

The Danish Council for Digital Security
Vester Farimagsgade 37B, 1. th., 1606 Copenhagen V
Telephone: +45 53 36 02 23 email: info@digitalsikkerhed.dk web: www.digitalsikkerhed.dk