Ministry of Justice and Security

> Return address Postbus 20301 2500 EH The Hague

European Data Protection Board

Information Management and Procurement Department

Turfmarkt 147
2511 DP The Hague
Postbus 20301
2500 EH The Hague
www.rijksoverheid.nl/jenv

Contact
Paul van den Berg

T 070 370 79 11

Our reference
3059243

Your reference
Public consultation reference 07/2020

Please quote date of letter and our ref. when replying. Do not raise more than one subject per letter.

Date 13 October 2020
Concerning Contribution to consultation by EDPB on the concepts of controller and processor in the GDPR

Introduction

The Dutch Ministry of Justice and Security acknowledges the importance of the interpretations and guidance given by the EDPB in the new Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Based on our experience as procurement officers for many different kinds of cloud services for the public sector, we would like to offer some general suggestions to clarify the role of cloud providers as data processors, in particularly globally operating cloud service providers. We also provide some specific text suggestions to add to the guidelines in the Appendix to this contribution.

Summary of recommendations

1. Distinguish between the role of a cloud provider of productivity and collaboration software concerning individual consumer end-users and the position concerning Business and Enterprise customers.
2. Explain in more detail why cloud providers, in principle, should operate as data processors for their Business and Enterprise customers, and not as (joint) data controllers.[1]
3. Explain for what purposes a data processor can and should process the personal data relating to the use of its services without becoming a (joint) controller.
4. Include a list of specific categories of personal data cloud providers generate, collect or otherwise process in their role as a data processor, not limited to the Customer Content Data.
5. Clarify the risks for data subjects in the case cloud providers are joint data controllers with their customers, as, in practice, it could leave gaps in the protection of the fundamental rights and freedoms of employees and other vulnerable data subjects

[1] SLM Microsoft Rijk is aware that cloud providers are under the GDPR not legally required to act as data processor. However, SLM Microsoft Rijk believes that instructing the cloud provider (by determining the purposes and means of the data processing) is the best approach, given the pratical cicrumstances, to safeguard the rights of data subjects.

6. Include a limitative set of circumstances and categories of personal data for the processing of which the cloud providers supplying to Business and Enterprise customers may act as (sole) data controllers.

About SLM Microsoft Rijk

We write in the role of Strategic Vendor Manager Microsoft for the Dutch government. We fulfil a crucial role in the public procurement of software products and services for all approximately 300.000 civil servants employed by the central Dutch government and the services and organisations that are part of the central government.

We started to commission DPIA reports in the summer of 2018. Although we are not a data controller ourselves, we commissioned those DPIAs to ensure we procure GDPR-compliant products and services for the Dutch government organisations. In practice, this often requires negotiations about technical and legal improvements.

Since the fall of 2018, we have published extensive DPIA reports on the main website of the Dutch government.[2] We have studied the role of Microsoft as the provider of the Enterprise versions of Microsoft Office (locally installed and as cloud software), of Microsoft Windows, of Microsoft Intune, and the role of Microsoft as the provider of data transfer and storage services (Microsoft Exchange Online, SharePoint, OneDrive and Azure).

Our role as a procurement department is not limited to Microsoft. We have also commissioned DPIA reports on G Suite Enterprise and G Suite Enterprise for Education, Amazon Web Services VM and database services, and the Zoom videoconferencing services. Besides, we are closely involved with the DPIA conducted by our colleagues from the Ministry of Economic Affairs on Oracle cloud services.

About The Hague Forum for Cloud Contracting

To share our findings with other public procurement officers in the EU, together with the EDPS, we helped found The Hague Forum for Cloud Contracting in 2019.[3] We have organised two meetings so far, on 19 August 2019[4] and on 2 July 2020. The Forum has over 100 members. We have learned from these meetings that there is a widely shared urgency to bundle forces and share data protection insights to ensure continued GDPR-compliant data processing while we shift infrastructure from *on-premise* to cloud-based data processing. Due to the Covid-19 pandemic, many public sector organisations find themselves in an uncomfortable split between the need to immediately deploy new cloud services to facilitate remote working and learning, and the need to carefully assess and negotiate GDPR compliance with globally operating cloud providers. We rely on the EDPB to provide much-needed guidance.

---

[2] See: https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise and https://www.rijksoverheid.nl/documenten/publicaties/2018/11/12/strategisch-leveranciersmanagement-microsoft-rijk-slm-microsoft

[3] https://thehagueforumforcloudcontracting.eu/

[4] An extensive report of the first meeting is available at: https://thehagueforumforcloudcontracting.eu/wp-content/uploads/2020/02/Article-on-EU-Software-and-Cloud-Suppliers-Customer-Council.pdf

The urgency of requested improvements
It is of critical importance that the EDPB provides clear and unambiguous guidance about the role of cloud providers, not only when they process personal data actively provided by their Enterprise customers, but also when they process other kinds of personal data generated and collected through the use of their services.

We call on the EDPB to provide an unequivocal explanation that cloud providers should operate as data processors for their Business and Enterprise Customer and that the cloud providers are in that case not at liberty to process the personal data about the use of services for their own (commercial) purposes.

This clarification is essential for two reasons:

1. To prevent joint controllership, as this leads to a lack of control over, and possibly unlawful further processing of, the personal data from employees and data subjects that interact with a business, government organisations and educational institutions in the EU.

2. To help data subjects exercise their fundamental data protection rights, such as accessing the personal data collected about their use of the service.

1. Prevent joint controllership
In our experience, most cloud providers only consider themselves a data processor for the specific personal data actively uploaded by their customers, the so-called Customer Content Data. In their contractual offerings to Business and Enterprise customers, they focus on their obligations and customers' rights concerning the processing of the Content Data. By omitting inclusion of arrangements for the processing of all other kinds of relevant personal data generated, collected or otherwise processed through the use of the services, customers may wrongfully assume their provider also acts as a data processor for these other kinds of personal data.

Customers have to figure out themselves that all categories of personal data not defined in such a data processing agreement, can be processed by the provider in a self-claimed role as a data controller. The provider can therefore assume it is contractually allowed to process these personal data for all purposes mentioned in a general, consumer-oriented, privacy statement. We have seen very unspecific and broad purposes in these statements such as: 'marketing', 'development of the services', 'research', 'future purposes for which we will ask consent', 'offering personalised recommendations', 'personalisation of the services', 'offering personalised advertising', 'processing for all purposes we deem compatible with the main purpose of providing the service', 'enrichment of personal data with external sources' and 'use of data as training sets for AI'.

To prevent obfuscation of the role of cloud providers as processor or controller, we recommend the EDPB to include a list of different categories of personal data processed by cloud providers, with an indication of the role of the provider. We provide a specific text suggestion in the Appendix.

As the EDPB explains in the sections 53, 62 and 63 of the draft guidelines, there is an inextricable link between the decision of an Enterprise customer to use a specific service from a cloud provider and the subsequent data processing by the cloud provider as a result of the use of the service. These *converging* decisions lead to a factual qualification as joint data controllers.

> *53. The situation of joint participation through converging decisions results more particularly from the case-law of the CJEU (...)* ***As such, an important criterion to identify converging decisions in this context is whether the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked. (...)***
>
> *62. It may also be the case that one of the entities involved provides the means of the processing and makes it available for personal data processing activities by other entities.* ***The entity who decides to make use of those means so that personal data can be processed for a particular purpose also participates in the determination of the means of the processing.***
>
> *63. This scenario can notably arise in case of* ***platforms, standardised tools, or other infrastructure allowing the parties to process the same personal data and which have been set up in a certain way by one of the parties to be used by others that can also decide how to set it up. The use of an already existing technical system does not exclude joint controllership when users of the system can decide on the processing of personal data to be performed in this context.***

However, the qualification as joint controllers leads to a highly undesirable situation, with an unequal balance of power. In an (undesired) role as joint controller, it is up to parties to negotiate an agreement. Business and Enterprise customers in the EU do not have enough leverage to negotiate GDPR-compliant agreements with most global cloud providers. As joint controllers, most organisations in the EU are not, or insufficiently, able to enforce compliance with transparency requirements, and impose restrictions such as data minimisation, purpose limitation, limitation of retention periods and, last not but least, to effectively allow data subjects to exercise their fundamental rights to access, correct and delete their personal data.
Business and Enterprise customers in the EU need to be able to refer to the obligations in Article 28 GDPR for data processors, to have the legal leverage to conclude GDPR compliant data processing agreements. The EDPB already helpfully explains in the current sections 38 and 81 of the guidelines that a cloud provider may still act as a data processor if it determines the data it needs to process for security purposes, and that a cloud provider may still be considered a data processor if, through the use of the service, it generates personal data relating to the service.

> *38. "Nonessential means" concern more practical aspects of implementation, such as the choice for a particular type of hard- or software or the detailed security measures which may be left to the processor to decide on.*

81. The EDPB notes that a service provider may still be acting as a processor ***even if the processing of personal data is not the main or primary object of the service,*** *provided that the customer of the service still determines the purposes and means of the processing in practice.*

We strongly recommend that the EDPB adds guidance for cloud providers in these guidelines so they generally cannot claim a role as a sole data controller. Although the actual role depends on the factual circumstances, in most cases, a self-qualification by the cloud provider as data controller would lead to a qualification as a joint controller with their Business and Enterprise customers.

As we explain in our publicly available DPIA reports, we do see some specific exceptions to the general rule that the cloud provider should act as a data processor of the personal data it obtains through the use of its services by Business and Enterprise customers.
A cloud provider can only legitimately act as a sole data controller in a very limited set of circumstances when the cloud provider necessarily has to process some personal data relating to the customer for its own legitimate business interests. Necessary means the provider has to pass a proportionality and subsidiarity test. In most cases, the cloud provider can suffice with the processing of aggregated data, for example, to create insights about the used resources and forecast required technical capacity. In other cases, the cloud provider has to process personal data from the customer, to send invoices or to check the validity of end-user licenses. We provide a longer list of these purposes in the Appendix with specific text suggestions.

2. Protect the rights and freedoms of employees and other vulnerable data subjects
Business and Enterprise customers of cloud providers can be small or large public sector or private sector organisations. They all need to facilitate the exercise of fundamental rights by two different categories of data subjects: their employees and all kinds of data subjects that interact with the organisation, be it voluntary or involuntary.

Employees generally do not have a choice to use another, more GDPR-compliant cloud service. Their employer typically offers the relevant work applications from a single supplier. System administrators equally have to perform their work duties within the cloud environment chosen by their employer. If the tools and services provided by the employers do not respect the fundamental rights to privacy and data protection, employees and data subjects that interact with information provided by the employers may incur high risks. These risks may vary from unlawful further processing of their personal data for unauthorised purposes to re-identification of pseudonymised data to an impossibility to exercise their right to access, correct or delete their personal data.

Other data subjects also lack a choice when they communicate through, for example, a website hosted by a cloud provider, or send an email that is processed by the recipient organisation in a cloud-based email service. If the communication with the organisation is involuntary, for example, if they are legally obliged to provide personal data to a government organisation, or when they have to take an exam through an online proctoring tool, they should be treated as a vulnerable group of data subjects.

Employees are in an unequal balance of power with their employer. Similarly, data subjects are sometimes required to provide personal data to a public sector organisation, through a service from a cloud provider. This means they are not free to consent to data processing by the cloud provider. Similarly, they are not free to negotiate individual contracts with cloud suppliers. However, many of the purposes described above for which cloud providers process personal data generated by the use of cloud services are based on the consent of the data subjects or a (fictive) contract between the end-user and the cloud provider.

Thus, in their self-claimed role as 'sole' data controllers, it is unclear on what legal grounds the cloud providers base their data processing. This cannot be solved by accepting joint controllership, as both parties still need to have their legal ground for data processing.

Inability to exercise the right to access

The problem with the self-claimed role of 'sole' data controller of a cloud provider is exacerbated by the impossibility for Business and Enterprise Customers to facilitate the exercise of data subjects rights.

In our DPIA practice, we use two methods to obtain access to the personal data generated, collected or otherwise processed by the cloud providers: (i) we file a formal Data Subject Access Request for our test data subjects, aimed at the cloud provider as data controller, and (ii) as the system administrator, we access all available log files the cloud provider makes available on behalf of our test data subjects.

It follows from our inspections that the cloud providers provide access to the personal Content data they collect in their role as data processors, but very little or no access to any of the other personal data they process in their self-claimed role as the data controller. Most cloud providers do provide access and correction rights concerning the Account and Contact Data, and some provide access and correction/deletion options for filed Support Requests. Still, so far, no cloud provider offers complete access to the different kinds of Diagnostic Data and Cookie Data they collect.

In our DPIA processes, we have heard the following reasons from cloud providers in their self-claimed role as data controllers not to grant full access to these personal data:

1. The data we collect are pseudonymous; we are not obliged to process additional information to identify the data subject for the sole purpose of complying with this Regulation (Article 11.1 of the GDPR).
2. It would require an unreasonable effort to identify the data subject (Article 11.2 of the GDPR).
3. We do not offer any possibilities to data subjects to provide additional information enabling identification because such access to these log files is strictly prohibited in our company to protect the rights of all data subjects, also from other customers (Article 23 sub i of the GDPR).

4. We do not offer access to our log files. We cannot provide an individual right to deletion, because this would infringe on our right (i) to use the data about all users to detect infringements and (ii) to keep secret what personal data we collect for security purposes as such information could be abused by malevolent actors (Article 23 sub i of the GDPR).

We think these arguments are often invalid and should be addressed by the EDPB. As data controllers, the cloud providers should design their systems in such a way (in line with recital 57 of the GDPR) that they facilitate digital identification of a data subject, for example through the authentication mechanism with the same credentials used by the data subject to log-in to the online service offered by the Business and Enterprise organisation. In our assessment, in principle, the cloud providers should only act as data processors for all personal data from Business and Enterprise customers processed through the use of their services. Based on Article 28(1) of the GDPR, they should implement the necessary technical and organisational measures to meet the requirements of this Regulation, including providing the means to the data controller to facilitate the exercise of fundamental rights by their employees and other data subjects.

In their role as data processors, the cloud providers should describe all categories of personal data they process on behalf of the controller. However, they may refrain from providing the full contents of all security logs, as long as they contractually agree that such data are only used for the specific security purpose, agree on data minimisation and a limited retention period.

APPENDIX: <u>Specific text suggestions</u>

1. Distinguish between the role of a cloud provider of productivity and collaboration software concerning individual consumer end-users and the role in relation to Business and Enterprise customers. This can be done by adding the following new section:

A distinction can be made between cloud services directly offered to consumers, and cloud services provided with volume licenses to Business and Enterprise customers (after this: organisations). However, many cloud services, developed initially for consumers, are now used by organisations to provide productivity, teleconferencing and other tools and environments to their employees for remote collaboration. In such circumstances, the provider of the cloud services should in principle only acts as data processor for the personal data they obtain, generate or derive directly or indirectly from the employees, customer and other data subjects that interact with the cloud service provided by the organisation.

2. Explain in more detail why cloud providers in principle, should operate as data processors for their Business and Enterprise customers, and not as (joint) data controllers. This can be done by adding the following new section:

Similarly, if a cloud provider has developed remote services aimed at organisations, such as flexible compute capacity, hosting of large file repositories and websites on virtual machines, use of virtual databases, or Artificial Intelligence platforms, the cloud provider should in principle only act as data processor for the personal data obtained directly or indirectly through the use of its services. If the cloud provider does not act, and contractually limit its role, as data processor, factually the cloud provider has to be qualified as joint controller with the organisations. This is a highly undesirable situation, as this requires the negotiation of detailed individual joint controller agreements and does not solve the problem that it is unclear on which legal ground(s) cloud providers rely for the processing of personal data of employees and other data subjects that may interact with these cloud services for their own purposes.

3. Explain for what purposes a data processor can and should process the personal data relating to the use of its services without becoming a (joint) controller. This can be done by amending and expanding the current section 63 into:

63. This scenario can notably arise in case of platforms, standardised tools, or other infrastructure allowing the parties to process the same personal data and which have been set up in a certain way by one of the parties to be used by others that can also decide how to set it up. Only data controllers are allowed under the GDPR to determine what personal data may be processed for what purposes. A data controller may use services from a technology company and outsource specific complicated data processing tasks, such as ensuring the security of the processing or providing a well-functioning, virtualised cloud hosting or collaboration service. To achieve such clear objectives, the data processor has certain liberty to decide how the personal data are processed, in which systems (with which means). Many cloud providers operate globally. For efficiency and security reasons, they provide a standardised infrastructure with standardised logging. They can still be qualified as data processors if they offer these services with a standardised data processing agreement if they limit the processing to activities that can and should be performed by data processors, such as:

1. *Technically providing a (remotely accessible) service;*
2. *Providing a well-functioning, bug-free and up to date service;*
3. *Securing the service*

However, if a processor exceeds the boundaries of this liberty, it factually acts as a data controller, and will also be qualified as a joint controller with the organisation that enables the processing by using this provider. The use of an already existing technical system may thus lead to joint controllership.

4. Include a list of specific categories of personal data cloud providers generate, collect or otherwise process in their role as a data processor, not limited to the Customer Content Data. This can be done by adding the following new section:

Cloud providers in their role as data processors should define, where applicable, the following categories of personal data they may generate, collect or otherwise process about the employees and other data subjects that interact with their services as used by organisations.

1. *Content Data (actively provided by customers, generally referred to as Customer Content, may include feedback on the content generated by the provider, such as rating);*
2. *Account Data (for example accounts of system administrators to manage the services, or end-user account data);*
3. *Contact Data (when separate from Account Data, for example, to contact salespersons);*
4. *Support Data (may include both Content Data and Diagnostic data about an issue/bug/error);*
5. *Financial Data (may include Account or Contact Data plus information about payments and some Diagnostic Data about used paid resources);*
6. *Diagnostic Data about the individual use of the service (may include telemetry data from end-user devices, data about system administrator behaviour, data about usage collected in security logs and data about end-users that access Content Data hosted on cloud infrastructures such as a virtual database or a website);*
7. *Cookie Data and similar technologies used on a publicly accessible website from the cloud provider (for example as an interface to read the privacy policy, read information about the capacities and pricing of the services);*
8. *Cookie Data and similar technologies used on a restricted access website from the cloud provider (for example as an interface for an admin to manage a cloud service, or to access support services).*

5. Clarify the risks for data subjects in the case cloud providers are joint data controllers with their customers, as, in practice, it could leave gaps in the protection of the fundamental rights and freedoms of employees and other vulnerable data subjects. This can be done by adding the following new section:

Employees are in an unequal balance of power with their employer. Similarly, data subjects are sometimes required to provide personal data to a public sector organisation, through a service from a cloud provider. This means they are not free to consent to data processing by the cloud provider. Similarly, they are not free to negotiate individual contracts with cloud providers. However, in their self-claimed role as data controllers, cloud providers tend to process the personal data for many purposes based on the consent of the data subjects, or based on a (non-existing) contract between the end-user and the cloud provider. Thus, in their self-assumed role as 'sole' data controllers, it is unclear on what legal ground cloud providers can rely for the data processing.

Based on Article 28(1) of the GDPR, cloud providers as data processors should implement the necessary technical and organisational measures to meet the requirements of this Regulation, including providing the means to the data controller to facilitate the exercise of fundamental rights by their employees and other data subjects. However, in practice, most cloud providers do not adequately help data subjects exercise their fundamental rights to access, correct and delete their personal data. Most cloud providers do not provide complete access to the different kinds of Diagnostic Data and Cookie Data they collect about the use of their services. They should either provide such access directly to the employees requesting such access, by allowing them to use the authentication mechanism with the same credentials they already use to log-in to the cloud service, or indirectly, by allowing the system administrators to download (a copy of the) processed personal data about the behaviour of the employees and other data subjects that have interacted with the cloud services provided by the organisation.
In their roles as data processors, the cloud providers should describe all categories of personal data they process on behalf of the controller. However, they may refrain from providing the full contents of all general security logs and refrain from deleting individual personal data, as long as they contractually agree that such data are only used for the specific security purpose, agree on data minimisation and a limited retention period.

6. Include a limitative set of circumstances and categories of personal data for the processing of which the cloud providers supplying to Business and Enterprise customers may act as (sole) data controllers. This can be done by adding the following new section:

Cloud providers sometimes need to process some personal data relating to their Business and Enterprise customers for their legitimate business interests. It is recommended that cloud providers include a separate list of purposes and personal data in their Data Processing Agreements for which they act as a sole data controller:

- *Financial Data for billing and preparing invoices;*
- *Account Data and/or Contact Data for account management, communicate with sales or procurement officials;*
- *Aggregated Financial Data for pricing, financial reporting and revenue calculations;*
- *Diagnostic Data to improve the core functionality, assess privacy compliance or energy efficiency of the cloud services;*
- *Diagnostic Data to combat fraud, cybercrime and cyber-attacks;*
- *Aggregated Diagnostic Data to assess usage of the services for business and capacity planning;*
- *Aggregated Financial and Diagnostic Data for product strategy, internal management reports and capacity forecasting;*

- *Content, Account, Contact, Support, Financial, Diagnostic and Cookie Data to comply with a legal disclosure order. This can only be invoked when the provider is forced to comply with a legal obligation from a non-EU country to hand-over personal data after having contested the order; the content is not protected by legal privilege, the provider is legally prohibited from forwarding the order to its Business or Enterprise customer and is legally prohibited from informing the customer or asking for an intervention by a National Supervisory Authority in the EU.*

Kind regards,

Paul van den Berg
Strategic Vendor Manager