



European Union Aviation Safety Agency

FO Personal data processing records and compliance checklist - Public

Ref # 073

Nr.	Item	Explanation
Use of Office 365		
1.	Last update of this record	31/03/2020
2.	Reference number	073
Part 1 – Article 31 of Regulation (EU) 2018/1725 - Record (recommendation: Publicly available)		
3.	Name and contact details of the controller and of the staff member responsible	Controller: European Union Aviation Safety Agency (EASA) Konrad-Adenauer-Ufer, 3 50452 Cologne, Germany Responsible staff member: Section Manager - IT Development, Security and Operations Email: servicedesk@easa.europa.eu
4.	Name and contact details of DPO	dpo@easa.europa.eu
5.	Name and contact details of joint controller (where applicable)	N/A
6.	Name and contact details of processor (where applicable)	Microsoft NV/SA, Da Vincilaan 3, B-1930 Zaventem, Belgium VAT registration number: BE 0437.910.359
7.	Purpose of the processing	Managing all office client applications at EASA and increasing the protection measures for the EASA identities.
8.	Description of categories of persons whose data are processed by EASA and list of personal data categories	Categories of persons whose data are processed by EASA: EASA staff members (including interims and consultants)





Categories of personal data processed:

Microsoft has published information about the minimal set of Personally Identifiable Information (PII) data required for each service to function.

EASA IT will aim to synchronize only the very least objects to the Microsoft cloud infrastructure. The project's scope is limited to the synchronisation of internal EASA accounts to the Microsoft Cloud and the deployment of Office applications to EASA's PC's.

The below data contains the minimum required data to make us of Office 365 applications out of a total of 162 attributes:

Attributes	Example value
accountEnabled	y/n
cn	Doe John
displayName	Doe John
objectSID	S-1-5-21-1202660629-329068152-682003330-2190
pwdLastSet	132191433935611400
samAccountName	Doejohn
sourceAnchor	Europe
usageLocation	Europe
userPrincipalName	john.doe@easa.europa.eu
mobile	+4912345678912





		In addition, diagnostic data and multifactor authentication data (i.e. sign-ins, audit logs and usage data) is processed.
9.	Time limit for keeping the data	<p>The data will be processed as long as the user stay's active as an EASA user.</p> <p>In EASA's leaver process the license for the Office 365 will be removed and the user disabled. Consequently, the personal data will be automatically deleted after 6 months. Multi Factor Authentication data (MFA i.e. sign-ins, audit logs and usage data) is kept for 30 days. However diagnostic data can be store up to 18 months according to this document.</p> <p>https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise/DPIA+Microsoft+Office+365+Online+and+Mobile+SLM+Rijk+23+july.pdf</p>
10.	Recipients of the data	<p>EASA IT will be the recipient of the data for all logging and event data.</p> <p>Microsoft processes data related to the functioning of the services but also usage data for the service.</p>
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	<p>As a cloud hosting and EU datacentre location was selected. According to MS this cloud is segregated from US cloud.</p>
12.	General description of security measures, where possible.	<p>Security Controls for the Client Installation:</p> <p>The privacy available under the Office 365 Pro plus software which is installed on EASA's computers allows the following privacy controls:</p> <p>https://docs.microsoft.com/de-de/deployoffice/privacy/overview-privacy-controls</p> <p>EASA decided on the following settings, whereby all telemetric and diagnostic sending of data is disabled.</p>





Settings	EASA decision
Diagnostic data sent from Office 365 ProPlus to Microsoft	<p>Disabled No diagnostic data about Office client software running on the user's device is collected and sent to us. This option, however, significantly limits our ability to detect, diagnose, and remediate problems your users may encounter using Office.</p>
Connected experiences that analyze your content	<p>Disabled - Connected experiences that analyze your content are experiences that use your Office content to provide you with design recommendations, editing suggestions, data insights, and similar features.</p>
Connected experiences that download online content	<p>Enabled - Connected experiences that download online content are experiences that allow you to search and download online content including templates, images, 3D models, videos, and reference materials to enhance your documents. For example, Office templates or PowerPoint QuickStarter. Microsoft tracks the use of these connected experiences according to https://docs.microsoft.com/en-us/deployoffice/privacy/connected-experiences</p> <p>According to https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise/DPIA+Microsoft+Office+365+Online+and+Mobile+SLM+Rijk+23+july.pdf the diagnostic data in O365 is stored for up to 28</p>





			months.	
		Other connected experiences	Disabled - In addition to the above there are some other connected experiences available in Office.	
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the below privacy statement.			





PRIVACY STATEMENT

USE OF O365 [Ref # 073]

1. What personal data do we collect?

Attributes	Example
accountEnabled	y/n
cn	Doe John
displayName	Doe John
objectSID	S-1-5-21-1202660629-329068152-682003330-2190
pwdLastSet	132191433935611400
samAccountName	Doejohn
sourceAnchor	Europe
usageLocation	Europe
userPrincipalName	john.doe@easa.europa.eu
mobile	+4912345678912

In addition, diagnostic data are processed.

Personal data are obtained from EASA Active directory. The EASA active directory is connected to the central HR database.





2. For what purpose do we collect personal data and on which legal basis?

With the usage of Microsoft Office 365 EASA is using the most modern available office application. It eases the overall client management and ensures continued deployment of new feature updates and increased protection against possible cyber threats.

The processing is based on Article 5(1)(a) and recital 22 of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data:

'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body'

'Processing of personal data for the performance of tasks carried out in the public interest by the Union institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies.'

The processing is also based on Article 75 of Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, which relates to the establishment and functions of EASA.

3. Who may receive your personal data?

EASA staff members from the IT department may receive your personal data.

The identity data gathered in cloud is being processed on the Microsoft Office 365 cloud. There is no function / individual receiving the personal data. The data is stored in the EU.

4. How long are your personal data kept?





Personal data is kept as long as the users have an active valid EASA account. In the EASA leaver process the account will be disabled on the day the user leaves. 6 Months after the leave the cloud account and the corresponding personal data will be automatically deleted. Multi Factor Authentication data (MFA i.e. Sign-ins, Audit logs and usage data) is kept for 30 days.

However diagnostic data can be stored up to 18 months.

5. What are your rights?

You have the right to request from EASA access to and rectification or erasure of your personal data or restriction of processing. You also have the right to object to processing of your personal data.

EASA should provide information on action taken on a request within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

A breach concerning your personal data should be communicated to you under certain circumstances. EASA should also ensure the confidentiality of electronic communications.

6. Who is the data controller and how to exercise your rights?

EASA should exercise the tasks of the data controller for the purpose of these processing operations.

To exercise the mentioned rights, you can contact the controller by sending an email to: servicedesk@easa.europa.eu

If you consider your data protection rights have been breached, you can always lodge a complaint with the EASA's Data Protection Officer (dpo@easa.europa.eu) or with the European Data Protection Supervisor: edps@edps.europa.eu.

