Record of processing activity

Processing data in the context of Microsoft 365 (M365) Services Guest access

Record of EBA activities processing personal data, based on Article 31 of Regulation (EU) 2018/1725 (EUDPR)

Nr	Item	Description
Part 1 - Article 31 Record (publicly available)		
1	Last update of this record	22/10/2021
2	Reference number	EBA/DPR/2021/5
3	Name and contact details of controller	Controller: European Banking Authority, Tour Europlaza, 20 avenue André Prothin, CS 30154, 92927 Paris La Défense CEDEX, France Contact: ExecutiveOffice@eba.europa.eu
4	Name and contact details of DPO	dpo@eba.europa.eu
5	Name and contact details of joint controller (where applicable)	Not applicable
6	Name and contact details of processor (where applicable)	Microsoft Ireland Operations Limited Microsoft EU Data Protection Officer[1] One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521 Ireland Telephone: +353 (1) 706-3117 https://aka.ms/privacyresponse A list of Microsoft's current sub processors is available at https://aka.ms/servicesapprovedsuppliers

[1] Reference: https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-data-protection-officer, accessed 27/07/2021.

Nr	Item	Description
7	Short description and purpose of the processing	The European Banking Authority (EBA) processes personal data to allow participants to access and use communication and collaboration functionality in the context of performing Agency tasks, including: Communication and collaboration using Microsoft Teams; Collaboration on documents using Microsoft SharePoint Online; Use of integrated Office 365 functionality within these tools.
8	Description of categories of persons whose data the EBA processes and list of data categories	Categories of persons: • Guest users - Natural persons outside EBA who are invited to collaborate on various EBA resources (e.g. data subjects from NCAs, ECB, ESMA, EIOPA). Categories of data: 1. **Identification data** is the guest user's email address (as depicted by the guest user's organization). This information is copied to all Office 365 data centres around the globe used to provide the service to allow global access and access control to the EBA's environment in Office 365. Identification data is visible to everyone having access to the EBA M365 environment. 2. **Content data** is any content uploaded to the Office 365 platform by users, such as documents (e.g. Word, Excel documents), and multimedia (e.g. video recordings). Such data is stored by in Office 365 but not otherwise processed by the service. 3. **Service generated data** contains information related to the usage of online services, which are the user IP address, creation time, site URL and user email address. This data is generated by events that are related to user activities in Office 365.

9	Time limit for keeping the data	• Identification data, i.e. guest user email address
		  ○ for as long as the guest user account is active, and
		  ○ 90 days after deletion of the guest user account
		• Content data
		  ○ up to 90 days upon expiration/termination of the subscription
		• Service generated data
		  ○ Until the business purposes for which the data was collected or transferred have been fulfilled

10	Recipients of the data	IT Unit administrators Information collected on Teams may, where necessary, be transmitted to the bodies in charge of monitoring or inspection tasks in accordance with European Union legislation.

Nr	Item	Description
		No personal data are transmitted to parties outside the scope mentioned herein, and neither Microsoft nor EBA share personal data with any other third party for any other purpose (e.g. direct marketing).
11	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	Yes, there are data transfers to third countries (see list of sub-processors under section 7). Transfer tools: • Adequacy decision for: Canada, Israel, Japan, UK and Republic of Korea (in the last steps of adoption). • Standard Conctractual Clauses, for the rest of the countries. Additional measures have been adopted (security controls – as shown in section 12).
12	General description of security measures, where possible	Organization, roles & responsibilities – EBA has defined data protection and information security responsibilities with the relevant powers and authorities.[2] • Information Security Framework EBA Information Security framework have been defined, approved by management, published, and communicated to EBA staff and contractors. They can be found in EBA's intranet Policies, Standards & Guidelines (europa.eu). Information Security Framework is complemented with information security controls that cover the following domains : asset management (responsibilities, ownership), information classification, media handling, access control, operations security (e.g. protection from malware, backup, logging & monitoring), communications security, system acquisition/development & maintenance, supplier relationships, information security incident management, information security aspects of business continuity management and compliance. • Physical Security Physical security controls exist in all EBA premises and they include access cards, badge readers, video surveillance and security guards. • Cyber Security Awareness All employees of the organization and, where relevant, contractors receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function. Moreover, EBA leverages a digital platform in this direction (KnowBe4). • M365 Security o Threat protection (Azure ATP Services, MFA);

[2] EBA/DC/2020/354 Decision of EBA concerning the roles of the Data Protection Officer and other EBA staff when processing personal data, and repealing Decision of the Management Board EBA DC 037

Nr	Item	Description

- Security management;
- Information Protection (DLP, AIP, Cloud App Security);
- Security management (secure score, security & compliance center, Azure Sentinel);
- Identity and Access Management;
- Privileged Identity Management (Azure AD);
- Encryption (in transit and at rest);
- Azure Key Vault (keys management) & custom keys;
- Endpoint management (Intune, MAM, MDM);
- Advanced compliance (Advanced eDiscovery, Customer Lockbox, Advance Data Governance, Service Encryption with Customer Key, Privileged Access Management).

- Dedicated Security Controls
  - Microsoft Advanced Threat Analytics, so that audit trails for EBA staff are adequately monitored.
  - Accountability on global administrators by assigning the relevant role at least at two physical persons, so that the one's actions could be auditable by the other party.
  - Third party application integration disable by default, so that only application with a clear value and security controls are granted access.
  - Advanced Threat Protection (ATP) Safe Links policy, so that sophisticated email attacks are being discovered, contained and mitigated.
  - Customer Lockbox. By enabling this feature, Microsoft technicians do not have access to EBA data unless approved by EBA for troubleshooting purposes.
  - SharePoint online classification policies, so that leakage of classified information is less likely to occur.
  - Awareness on EBA staff regarding permissions on files/folder/sites sharing on MS Teams and SharePoint.
  - Common Attachment Types Filter, so that a user can block known and custom malicious file types from being attached to emails.
  - Exchange Online Spam policies.

Nr	Item	Description

- Prohibit whitelisting of specific domains, so that malicious domains cannot bypass anti-spam controls.
- Prohibited Client Rules Forwarding, so that clients cannot manage auto-forwarding in EBA tenant.
- Disable of basic authentication, so that are not granted access.
- Email protection controls: DKIM, SPF, and DMARC.
- Exchange Online Protection, so that administrators are notified for outgoing malicious email traffic.
- M365 audit logs, so that O365 back office teams can investigate activities for regular security operational or forensic purposes.
- Mailbox auditing, so that Microsoft 365 back office teams can track logons to a mailbox as well as what actions are taken while the user is logged on.
- Regular reviews of:
  - Application Usage report, so that operators can have a knowledge of risky apps that users have enabled, causing data spillage or accidental elevation of privilege.
  - User role group changes, so that no one has been improperly added to an administrative role.
  - Mail forwarding rules, so that no unauthorized domains have been added to them.
  - Malware detections report, so that a sense of the overall volume of malware being targeted at EBA users is received.
  - Account provisioning activity report, so that unusual third party applications are being spotted.
  - Non-global administrator role group, so that special privileges cannot be used illicitly.
  - Blocked users for spamming, to identify whether those users have been targeted, or their accounts have been compromised.
- Spoof Intelligence, to gain an understanding of senders who are spoofing either domains that are part of your organization, or spoofing external domains.
- Sign-in risk policy, so that suspicious sign-ins are challenged for multi-factor authentication.

Nr	Item	Description
		• Data Encryption in transit and at rest • Pseudonymized identifiers • Data access • Right to audit • Security incident notification • Sub-processors security
13	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:	A link to the relevant privacy notice is being included to the registration email sent to the guest users.