Record of Personal Data Protection of Personal Data Processing Activity, pursuant to Article 31 of Regulation (EU) 2018/1725[1]

Visitor management system

I. GENERAL INFORMATION

1) Contact Details of Controller(s) (Note 2)
Name: European Banking Authority (EBA), represented by the Corporate Support unit Email Address: meetings@eba.europa.eu

2) Contact Details of Processor *Who is actually conducting the processing?*
Name/Data Protection Coordinator's Name: Proxyclick Email Address: legal@proxyclick.com Date: 19/08/2020

II. DESCRIPTION & PURPOSE OF PROCESSING

3) Description of Processing (see Note 3)
We will implement a software tool that allows us to register visitors and contractors in the tool. The tool will generate e-mail invitations with a unique code they can use to check-in/out on the tablets we will have available at reception. We will use the information from the meeting registration forms in the extranet, directly obtained from visitors/contractors at reception or from their EBA hosts.

[1] 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

4) Purpose of processing (see Note 4)

Why are the personal data being processed?

Specify the rationale and underlying reason for the processing

☐ Staff administration

☒ Relations with external parties

☒ Procurement, finance and accounting

☐ Administration of membership records

☒ Auditing

☒ Information administration

Other (please give details):
This tool will streamline and speed-up the check-in process of visitors reducing the time at reception, considered a risk-zone given the Covid-19.

5) Lawfulness of Processing

Article 5 of Regulation (EU) 2018/1725

A. Legal Basis justifying the processing:

Under the umbrella of article 5 from Regulation (EU) 2018/1725, our legal basis to process the data are as follows:
1.(a) 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; controlling their presence on our premises is essential for their security as well as of our own staff, and required to verify on their eligibility to certain reimbursements or allowances.
1.(d) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; the visitors consent to provide their data so we can host them in our premises and offered them certain services (e.g. catering).

B. Processing is necessary:

☒ for the performance of a task carried out in the public interest

☐ for compliance with a legal obligation to which the Controller is subject

☐ for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

☐ in order to protect the vital interests of the data subject or of another natural person

Or

☒ Data subject has given his/her unambiguous, free, specific and informed consent

III. CATEGORIES OF DATA SUBJECTS & PERSONAL DATA

6) Categories of Data Subjects (see Note 5)

Please tick all that apply and give details where appropriate

☐ EBA Temporary Agents or Contract Agents

☐ SNEs or trainees

☒ Visitors to the EBA (BoS, MB, Working Groups, Sub-Groups, Seminars, Events, other)

If yes, please specify: All visitors attending to the premises

☒ Providers of good or services

☐ Complainants, correspondents and enquirers

☒ Relatives and associates of data subjects

Other (please specify):

7) Categories of personal data (see Note 6)

Please tick all that apply and give details where appropriate

(a) **General personal data:**

The personal data contains:

☒ Personal details (name, surname, email, phone number, country of employment, picture)

☐ Education & Training details

☒ Employment details (name of employer, function)

☐ Financial details

☐ Family, lifestyle and social circumstances

Other (please give details) :
Time of check-in and check-out from the premises.

(b) **Special categories of personal data:**

The personal data reveals:

☐ Racial or ethnic origin

☐ Political opinions

☐ Religious or philosophical beliefs

☐ Trade union membership

☐ Genetic or Biometric data

☐ Data concerning health, sex life or sexual orientation

Important Note
If you have ticked any of the sensitive data boxes contact the Data Protection Officer before processing the data further.

IV. CATEGORIES OF RECIPIENTS & DATA TRANSFERS

8) Recipient(s) of the data *To whom is the data disclosed?*
☐ Managers of data subjects

☒ Designated EBA staff members

☐ Relatives or others associated with data subjects

☐ Current, past or prospective employers

☐ Healthcare practitioners

☐ Education/training establishments

☐ Financial organisations

☒ External contractor

Other (please specify):

Auditors

9) Data transfer(s)

Is the data transferred outside the EBA?

☐ Within the EBA or to other EU Institutions/Agencies/Bodies

If yes, please specify:

☒ To other recipients within the EU (e.g. NCAs)

☐ To third countries

If yes, please specify:

a) the country:

b) whether suitable safeguards have been adopted:

Adequacy Decision of the European Commission[2] ☐

Standard Contractual Clauses ☐

Binding Corporate Rules ☐

Administrative Arrangements between public Authorities ☐

☐ To international organisations

If yes, please specify the organisation and whether suitable safeguards have been adopted:

Important Note

If no safeguards have been put in place, please contact the DPO before processing the data further.

V. RETENTION PERIOD & SECURITY MEASURES

[2] Third countries for which the European Commission has issued adequacy decisions are the following: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

10) Retention period (see Note 7)

A. How long will the data be retained and what is the justification for the retention period?

Data will be kept for 18 months from collection. This period should suffice to process any payment or reimbursement request from which the confirmation of presence at EBA premises is required.

B. For further processing envisaged beyond the original retention period for historical, statistical or scientific purposes, please specify whether the personal data will be anonymised:

☒ No

☐ Yes

11) Storage media & security of processing

A. Please indicate how and where the data processed are stored
(e.g. Share Point / cloud):
Data is processed in course of providing cloud based (SaaS) visitor management system and stored in servers located in France and Germany

B. Technical & Organisational Security measures adopted:

☒ Controlled access to ICT-system/controlled access codes

Access to the Proxyclick production network is restricted by an explicit need-to-know basis, utilizing least privilege. It is audited and monitored frequently, and controlled by our Management Team. Employees accessing the Proxyclick production servers are required to use multiple factors of authentication.

☒ Restricted access to physical location where data is stored

Live customer data is only stored at AWS and OVH data centers which are certified and have strong physical security measures, e.g. barbed wire fences, video surveillance, motion detection systems, surveillance team on site 24/7/365

☒ Pseudonymisation and Encryption

Communications between you and Proxyclick servers are encrypted via industry best practices: HTTPS and Transport Layer Security (TLS) over public networks. The hard disks of all servers are encrypted. Databases on the client iPads are also encrypted.

☒ Back-up

Audit trails include the time of change made to a visit, the user that performed the change, and the content of the change. Changes to data by users are logged in audit trails. Audit trails contain the time of change, the user that performed the change and the content of the change

☒ Audit trails

Audit trails for infrastructure changes are automatically generated

☒ Confidentiality agreement/clause

Both employees and vendors are subject to relevant confidentiality obligations.

☒ Test the effectiveness of security measures adopted

In addition to Proxyclick's extensive internal scanning and testing program, penetration tests are performed by selected clients on an ad hoc basis. Proxyclick also employs third-party security experts to perform a broad penetration test across the Proxyclick service offering annually.

☒ Training of staff

Employees are trained at least annually on privacy and information security matters. Furthermore, engineers participate in secure code training covering OWASP Top 10 security flaws, common attack vectors, and Proxyclick security controls.

Other (please specify):
For further information please see here or the technical and organizational security measures set out in the DPA.

Consultation of the Data Protection Officer
Email Address: dpo@eba.europa.eu Date of consultation: 23/09/2020 Date of approval of processing: 30/09/2020

Privacy statement available at: available internally

Date of insertion in Register: 30/09/2020

Guidance Notes

Note 1

Enter here the name of the processing operation involving personal data (e.g. staff recruitment, business continuity contact list)

Personal data is any information relating either directly or indirectly to a living identified or identifiable person. This information may, for example, be the name, date of birth, a telephone number, biometric data, medical data, professional details, etc.

Processing means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Note 2

In case of more than one controller (i.e. joint processing operations), all controllers need to be listed.

Note 3

Enter any details of the processing operation that are not clear from the name of the operation entered above.

Note 4

Personal data must only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those processes.

Note 5

The data subject is an identified or identifiable natural person who is the subject of the personal data.

Note 6

According to Article 10 of Regulation (EU) 2018/1725, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, as well as of genetic and biometric data, and data concerning health and sex life or sexual orientation, is generally prohibited but exemptions may apply.

Note 7

Personal data should be kept for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.