

PRIVACY NOTICE

Data are processed pursuant to the provisions of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: "General Data Protection Regulation"), and Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter: "Privacy Act").

It is in the interest of OTP Bank Plc. (hereinafter: "Bank") to develop its human resources by providing the knowledge needed for the achievement of the objectives of both the Bank and the Group, and for individual self-improvement efforts. To this end, it organises and delivers training courses, implements training processes, supports them with IT systems, and keeps records of and retrieves the necessary data.

The Bank may also train employees of the Banking Group's subsidiaries and partners for its own purposes or those of the Group.

This Privacy Notice shall only apply to processing activities carried out by the Bank acting as controller. In the event that a subsidiary of the Banking Group uses the training system as controller, the Bank shall be considered the processor and this Privacy Statement shall not apply to the processing carried out by the subsidiary.

The following tables summarise the main features of data processing under this Notice:

1. THE INDIVIDUAL PROCESSING OPERATIONS

1.1. Organisation and delivery of training in the Training Module

The Bank organises and delivers training courses in its Training Module which includes the SuccessFactors (hereinafter: "SF") Learning Management System (hereinafter: "LMS") and the Training Portal. The Bank implements training processes and events and keeps records of data in each system. Organising and delivering training courses naturally entails the processing of personal data.

For subsidiaries of the Banking Group, and partners, training can also be delivered through SF LMS or the Training Portal. Data may be processed by either only the Training Portal or the Training Module (i.e. both by the SF LMS and the Training Portal). This is determined by where the training is delivered from and where the data subject is accessing from. If accessing from the Training Module, the data subject will log in through the Training menu in the SF system. If accessing from the Training Portal, the data subject will log in via elearning.otpbank.hu. In this case, SF LMS will not process the data subject's data.

PURPOSE OF PROCESSING	LEGAL BASIS FOR PROCESSING	SCOPE OF DATA PROCESSED	DATA RETENTION PERIOD
Organising and delivering training courses in the Training Module.	Legitimate interest [Article 6(1)(f) of the General Data Protection Regulation (GDPR)].	BANK EMPLOYEES AND EMPLOYEES OF THE BANKING GROUP'S SUBSIDIARIES ACCESSING THROUGH THE SF SYSTEM, PARTNERS: <u>Data on training participants:</u> Identification data: name, academic degree/prefix, registration number, work email address, status, manager. Occupational and organisational information: job title, status (active / inactive), code of absence and its duration, secondary function, location, country, place of work, organisation (company, division / region, department / branch, division), branch category, branch code, cost centre, date of entry and exit, personnel group, type of employment, name and registration number of line manager. Information on user rights, access and user group, role. Information on assigned training courses, curriculum and programmes, training history, completion. Information on participant registration and participation.	For bank employees, 5 years after the termination of their employment or, for training under the Adult Education Act, 8 years after the last training, whichever is later. For employees of the Banking Group, 5 years after the last training or, for training under the Adult Education Act, 8 years after the last training, whichever is later. For partners, 5 years after the termination of their legal relationship or, for training under the Adult Education Act, 8 years after the last training, whichever is later.

		Information on access to content elements of online training courses. Information on the questionnaires to be completed. Information on approvals in the system. Data on badges earned. <u>Data on instructors:</u> Name, academic degree/prefix, company, role, organisation, email address, comments, CV, associated user, user rights, training start and end date and time, tool booking, training description. <u>Data on other users:</u> Name, academic degree/prefix, registration number, role, work email address, status, organisation, information on user rights and access. Information on user groups. With regard to the above data, the data included in individual reports. Data related to logging.	
		EMPLOYEES OF THE BANKING GROUP'S SUBSIDIARIES ACCESSING THROUGH THE TRAINING PORTAL, SPECIFIC PARTNERS WHOSE TRAINING TAKES PLACE EXCLUSIVELY THROUGH THE TRAINING PORTAL: Identification data: name, academic degree/prefix, registration number, work email address / email address. Country, job title, place of work, company, organisation (division, directorate, department / branch), telephone number. Information on user rights, access and user group, role. Information on assigned training courses, curriculum and programmes, training history, completion. Information on participant registration and participation. Information on access to content elements of online training courses. Information on the questionnaires to be completed. Data on badges earned. <u>Data on persons in specific roles:</u> name, academic degree/prefix, registration number, work email address / email address, assigned course, role.	For employees of the Banking Group, 5 years after the last training or, for training under the Adult Education Act, 8 years after the last training, whichever is later. For partners, 5 years after the termination of their legal relationship or, for training under the Adult Education Act, 8 years after the last training, whichever is later.

1.2. Training courses under the Adult Education Act (if the Bank is the adult education provider)

Certain training courses are organised and delivered under Act LXXVII of 2013 on Adult Education (hereinafter: "Adult Education Act") and its implementing Government Decree No. 11/2020 (II. 7.) (hereinafter: "Implementing Decree"). This legislation provides for the conclusion of an adult education contract, keeping records of data, the scope of data to be processed, its retention period and reporting in the Adult Education Reporting System for the Bank acting as an adult education provider. When organising and delivering training courses, in addition to the data set out in Section 1 above, the data required by the Adult Education Act shall also be provided.

PURPOSE OF PROCESSING	LEGAL BASIS FOR PROCESSING	SCOPE OF DATA PROCESSED	DATA RETENTION PERIOD
Meeting the record-keeping obligation under the Adult Education Act, organising and delivering training courses. Issuing certificates of training courses.	Meeting a legal obligation [Article 6(1)(c) of the General Data Protection Regulation (GDPR)]: pursuant to Sections 16 and 21 of the Adult Education Act and Sections 21–22 of the Implementing Decree.	<u>Pursuant to Section 21 of the Adult Education Act:</u> <u>Data on training participants:</u> natural person identification data (name and surname, name and surname at birth, place and date of birth, mother's name and surname at birth¹), email address, highest educational attainment, data in the document certifying the completion of a training activity, education identification number, vocational qualification, vocational training, foreign language skills, entry into training, completion of training, or, failing this, exit from training, data concerning assessment and certification during training and payment obligation related to training. <u>Pursuant to Section 16 of the Adult Education Act:</u> <u>Data on training participants:</u> Data on attendance. Contents of documents certifying compliance with the prerequisites of entering and participating in education and training, initial competence assessment, contents of documents certifying prior knowledge assessment. <u>Data on instructors:</u> Contents of documents relating to the employment of instructors. <u>Pursuant to Section 21 of the Implementing Decree:</u> <u>Contents of the adult education contract:</u> The name of and number of sessions in the training, the start and end dates of the training by year, month and day, progress schedule broken down by units of study, indication of the document to be obtained by completing the training, how training performance is monitored and assessed, and, if the training concludes with an exam, the conditions for taking such exam, the number of absences allowed and the consequences of exceeding that number for the training participant, the amount of the training fee and the method of its payment, the amount of the training grant broken down by budgetary and EU funds, the consequences of breach of contract by the training participant and by the adult education provider.	For employees of the Bank: 5 years after the termination of their employment or 8 years after the last training, whichever is later. For employees of the Banking Group, and partners: 5 years after the last training or 8 years after the last training, whichever is later.

¹ Pursuant to Section 4(4) of Act XX of 1996 on Means of Identification Replacing the Personal Identity Number and on the Use of Identification Codes.

		Pursuant to Article 22 of the Implementing Decree: <u>Contents of the certificate:</u> certificate serial number, name and registration number of the adult education provider, the training participant's name and surname, name and surname at birth, place and date of birth, mother's name and surname at birth, name, date and number of sessions in the training, place and date of issue of the certificate, name and position of the issuer of the certificate.	
--	--	--	--

1.3. Use of photos on the Training Portal

Users can upload photos to the Bank's Training Portal at their discretion. By uploading photos, users consent to processing.

PURPOSE OF PROCESSING	LEGAL BASIS FOR PROCESSING	SCOPE OF DATA PROCESSED	DATA RETENTION PERIOD
Using a photo on the Training Portal: improving user experience, enhancing personalisation, enabling mutual recognition.	Consent [Article 6(1)(a) of the General Data Protection Regulation (GDPR)] Voluntary and optional!	Image.	For employees of the Bank: Until the withdrawal of consent or the end of the month following the year when the employment is terminated. For employees of the Banking Group's subsidiaries, and partners: Until the withdrawal of consent or the end of one year after the last training.

2. DETAILS OF THE CONTROLLER AND THE CONTROLLER'S DATA PROTECTION OFFICER

Controller's name: OTP Bank Plc. (registered office: H-1051 Budapest, Nádor utca 16; company registration no.: 01-10-041585; postal address: OTP Bank Nyrt., H-1876 Budapest; email address: informacio@otpbank.hu; phone number: (+36 1/20/30/70) 3 666 666; website: www.otpbank.hu)
Data Protection Officer's name: Zoárd Gázmár (postal address: H-1131 Budapest, Babér u. 9; email address: adatvedelem@otpbank.hu)

3. SCOPE OF DATA SUBJECTS

Employees of the Bank and the Banking Group's subsidiaries whose data are processed in their respective roles in relation to the organisation and delivery of a training event.
Partners of the Bank whose data are processed in their respective roles in relation to the organisation and delivery of a training event.
Instructors whose data are processed in relation to the organisation and delivery of a training event.

4. DATA SOURCES

Sources of the personal data processed in relation to the purposes of processing are the data subject, the Bank's systems, the Bank's departments and the Banking Group's subsidiaries.

5. RECIPIENTS OF PERSONAL DATA

SF LMS is supplied by SAP Hungary Kft. (company registration no.: 01-09-667656; registered office: H-1031 Budapest, Záhony u. 7), which acts as a processor in the course of its activities.
SF LMS is supported by BCS Business Consulting Services Kft. (company registration no.: 01-09-280530; registered office: H-1118 Budapest, Rétköz u. 5), which acts as a processor in the course of its activities.

The processor may process personal data only in line with the instructions of the Bank and has no autonomous decision-making powers with regard to processing. The processor undertakes a non-disclosure obligation and contractual safeguards in respect of the protection of the personal data accessed by it during the performance of its tasks.

The Bank shall transfer the data set out in Section 15 of the Adult Education Act (name, nature, place, number of session in, first day, planned date of completion of education and training, natural person identification data of training participants (name and surname, name and surname at birth, place and date of birth, mother's name and

surname at birth²), email address, highest educational attainment, training fee and the person responsible for paying it, in certain specific cases an education/training schedule for progress by training group, broken down by date, time and place and number of sessions, and the planned date of completion) as well as certificates and the data included therein as provided for in Section 22 of the Implementing Decree to the Adult Education Reporting System; the Pest County Government Office is responsible for keeping records, acting as an independent data controller within the scope of its duties and powers.

6. DATA SECURITY

The IT systems and other data storage facilities of the Bank are located at its registered office and on the servers leased by the processor. The Bank selects and operates the IT tools used to process personal data during the provision of the service in such a way that the data processed are:

- accessible to the authorised persons (availability);
- credible and authenticated (authenticity);
- verifiably unchanged (data integrity);
- protected from unauthorised access (confidentiality).

We take particular care to ensure data security, and take all technical and organisational measures and adopt procedural rules required for enforcing the safeguards specified in the General Data Protection Regulation. We take appropriate measures to protect the data from unauthorised access, alteration, transfer, public disclosure, deletion or destruction, as well as damage and accidental loss, and ensure that the data stored cannot be corrupted or rendered inaccessible due to any changes in or modification to the applied technique.

The IT systems of the Bank and our partners are protected from computer-assisted fraud, computer viruses, hacking and distributed denial-of-service attacks. Moreover, the operator ensures security by means of server-level and application-level security procedures. Data are backed up on a daily basis. Our company takes all possible measures to prevent personal data breaches and in the event of a data breach it takes action immediately to minimise the risks and eliminate the damages.

7. THE DATA SUBJECT'S RIGHTS AND LEGAL REMEDIES IN CONNECTION WITH THE PROCESSING

Pursuant to Articles 12–21 of the General Data Protection Regulation, data subjects may request from the Controller access to and rectification or erasure of their personal data as well as the restriction of processing; moreover, they have the right to object to the processing.

In the event of a violation of their rights defined in the General Data Protection Regulation, data subjects may lodge a complaint with the Controller at the contact details specified in Section 1.

You, as a data subject, have the following rights:

7.1 Right of access

You have the right to be informed about whether we process your personal data as well as the right to know the following information:

- purpose or purposes of processing;
- the categories of the personal data processed;
- recipients to whom we transfer your personal data, with special regard to cases where your personal data are transferred to a third country or to international organisations;
- envisaged duration of the processing of your personal data;
- the administrative and judicial bodies where a complaint can be lodged;
- origin of personal data if they are not provided directly by you;
- whether your personal data are subject to automated processing, that is, a procedure where the personal data are used to evaluate, analyse or predict certain personal characteristics related to you. Such personal characteristics may concern your performance at work, your economic situation, health condition, personal preferences, interests, reliability, behaviour, location or movements.

On one occasion, you may request a complimentary copy of the personal data undergoing processing, and if you make the request by electronic means, you have the right to receive the information in a commonly used electronic form, unless you request otherwise and the Controller is capable of providing the data in that format. Please be advised that we may reject your request for a copy if this may adversely affect the rights and freedoms of other data subjects.

² Pursuant to Section 4(4) of Act XX of 1996 on Means of Identification Replacing the Personal Identity Number and on the Use of Identification Codes.

7.2 Right to rectification

You shall have the right to obtain from the Controller without undue delay the rectification of inaccurate personal data concerning you. Taking into account the purposes of processing, you also have the right to have incomplete personal data completed.

7.3 Right to erasure

You have the right to obtain from the Controller without undue delay the erasure of personal data concerning you. The Controller shall have the obligation to erase your personal data without undue delay where one of the following grounds applies:

- the personal data are no longer needed for the purposes for which they were collected or otherwise processed;
- you withdraw your consent, and there are no other legal grounds for the processing;
- the legal basis for processing is a legitimate interest, a public interest or the exercise of official authority, and there are no overriding legitimate grounds for the processing;
- where personal data are processed for direct marketing purposes, you have the right to object at any time to processing of the personal data concerning you for such purposes;
- the personal data were unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation under Union or Member State law to which the Controller is subject;
- the personal data have been collected in relation to children under 16 years of age and in relation to offering services related to information society.

The request for erasure cannot be complied with if the processing is necessary. Processing is deemed necessary for the following objectives:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing by Union or Member State law to which the Controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
- for health or occupational health purposes or for reasons of public interest in the area of public health;
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the erasure of personal data is likely to render impossible or seriously impair the achievement of the objectives of that processing;
- for the establishment, exercise or defence of legal claims.

7.4 Restriction of processing (blocking)

You have the right to obtain from the Controller restriction of processing where one of the following applies:

You contest the accuracy of your personal data, in which case the restriction applies to a period that enables the Controller to verify the accuracy of such personal data;

- the processing is unlawful, but you oppose the erasure of the personal data and request the restriction of their use instead;
- the Controller no longer needs the personal data for the purposes of the processing, but they are required by you for the establishment, exercise or defence of legal claims; or
- the legal basis for processing is a legitimate interest, a public interest or the exercise of official authority, and you object to the processing;
- in which case the restriction remains in force until it is determined whether the legitimate grounds of the Controller override your legitimate grounds.

7.5 Objection to processing

You have the right to object at any time, on grounds relating to your particular situation, to the processing of your personal data if the processing is based on a legitimate interest, a public interest or the exercise of official authority, including profiling. In such a case, the Controller can no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, you have the right to object at any time to processing of personal data concerning you for such marketing, which includes profiling to the extent that it is related to such direct marketing. In this case, personal data may no longer be processed for such purposes.

You may also exercise the right to object by automated means using technical specifications.

Where personal data are processed for scientific or historical research purposes or statistical purposes, you, on grounds relating to their particular situation, have the right to object to processing of personal data concerning you, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

7.6 Enforcement

Moreover, data subjects may lodge complaints with the National Authority for Data Protection and Freedom of Information (<http://naih.hu>; H-1055 Budapest, Falk Miksa u. 9–11.; postal address: H-1363 Budapest, Pf.: 9; phone: +36 1 391 1400; fax: +36 1 391 1410; e-mail: ugyfelszolgalat@naih.hu). Data subjects are entitled to lodge

OTP Bank Plc.

Website: www.otpbank.hu

Registered office:

H-1051 Budapest, Nádor utca 16.

Company Registry Court of the Budapest-Capital Regional Court:

10-01-041585

complaints with other supervisory authorities, in particular with those established in the Member State of their habitual place of residence.

A lawsuit may also be brought against the Controller for the violation of the rules applicable to the processing of personal data. Data subjects may bring the lawsuit before the Budapest-Capital Regional Court or the regional court having jurisdiction over their place of residence. The contact details of the regional courts in Hungary are available at: <http://birosag.hu/torvenyszekek>. If the habitual place of residence of the data subject is in another EU Member State, the action may be brought before the court of the competent jurisdiction in the Member State where their habitual residence is located.