UBS

CANDIDATE PRIVACY NOTICE – MONACO

DATA PROTECTION UNDER THE LAW NO. 1.565 OF DECEMBER 3 2024

To run our business, UBS collects and uses information about living individuals ("**Personal Data**"), including information about our current, former and prospective candidates for employment with UBS ("**you**")**.**

UBS takes your privacy seriously. This Candidate Privacy Notice ("**Notice**") contains information on what Personal Data the UBS employing entity ("**UBS**", "**we**", "**our**", or "**us**", see relevant UBS entities in section 10) and other companies of the group to which we belong (the "**UBS Group**") collect(s), what they do with that information, and what rights you have.

As part of our commitment to protect your Personal Data we want to inform you in a transparent manner:

- why and how UBS collects, uses and stores your Personal Data;
- the lawful basis for the use of your Personal Data; and
- what your rights are in relation to such processing and how you can exercise them.

Table of Content	
1 What does this Notice cover?	6 How long do we store your data?
2 What type of Personal Data do we collect?	7 What are your rights and how can you exercise them?
3 For which purpose do we process your Personal Data and what legal basis do we rely on?	8 Changes to your Personal Data
4 How do we protect Personal Data?	9 Updates to this Notice
5 Who has access to Personal Data and with whom are they shared?	10 List of UBS employing entities covered by this Notice

1 What does this Notice cover?

This Notice applies to any and all forms of use of Personal Data ("**processing**") by us in Monaco if you are a current, former or prospective candidate of any of the UBS employing entities listed in section 10.

2 What type of Personal Data do we collect?

For prospective, current and former candidates, we collect basic identification information, such as your name, title, position, professional history, experience and contact details.

If you actively apply for a role with UBS, we will usually also collect:

- Personal details and identification information (e.g., date of birth, nationality, picture, gender, ID card, passport numbers and other national ID numbers as required, immigration status);
- Physical and electronic address details (e.g., private telephone number, private email and/or postal address and business telephone number);
- Education and employment information (e.g., remuneration at your current employer, employment dates with your current employer, interview performance evaluation and scores in any online testing, position information such as position title, and language skills);
- Information submitted as part of your application (e.g., recordings of any video interviews in which you participate, and anything you choose to submit by choice in support of your application);

- Electronic and physical communication information, including but not limited to in- and outbound emails including attachments, phone conversations, chat or other instant messaging, faxes (digital) and other communication data (e.g., phone meta data);
- Where relevant, behavioural information and information about personality traits such as data collected to assess a candidate's suitabilty; and
- Where relevant and to the extent permitted by applicable law, the Personal Data that we collect will also include data about alleged or proven criminal convictions and offences.

Information you submit as part of your application must be true, accurate, complete and not misleading. Any false or misleading statements or omissions made by you during the application process, including your application and any assessments and interviews, may be sufficient cause to justify the rejection of your application or, if you have already become an employee, the immediate termination of your employment, subject to due process.

If you provide information about your family or any other third party to us as part of your application (e.g., emergency contacts or referees) then, before providing us with such information, you must inform the relevant individuals that you will disclose their Personal Data to us and provide a copy of the information in this Notice to them.

If you accept a role with UBS, then in order to conduct any necessary background checks and create your record in the UBS Group employee database, we will usually also collect:

- Family information (e.g., marital status, and details of any family or personal relationships within UBS); and
- Financial information (e.g., summary credit history, bank account details, tax-related information, and information required to undertake required checks for money laundering, criminal activities, corruption, terrorist financing and related matters).

In some cases, the Personal Data we collect from you is needed to meet our legal or regulatory obligations. If so, we will indicate to you that the provision of this information is mandatory, and the consequences if we cannot collect this information.

We may use cookies, tracking technologies and other means (e.g., web beacons, pixels, gifs, tags, unique identifiers) to collect and process the above information from different channels and devices you use, including email, and devices that you use to interact with us to access UBS websites, UBS platforms, products, services and applications for mobile devices.

For our usage of cookies and other tracking technologies in relation to UBS websites please also refer to the UBS Website, Social Media and Cookie Notice available here.

The above-mentioned Personal Data are collected from information that you directly provide (through the completion and submission of online application forms and profiles, through resumes or curriculum vitae, or through interviews or other communications). In some cases, UBS will also collect Personal Data indirectly from third parties, such as recruitment agencies that you used to apply to UBS, background check providers such as HireRight or Sterling and other administration services providers (for instance who provide candidate shortlisting services), or from publicly available sources such as business- and employment-orientated social networking services and job boards.

3 For which purposes do we process Personal Data and what legal basis do we rely on?

3.1 Purposes of processing

We always process your Personal Data for a specific purpose and only process the Personal Data which is relevant to achieve that purpose. In particular, we process Personal Data of candidates, within applicable legal limitations, for the purposes of:

a) Recruiting and application handling:

- to undertake recruitment activities, such as determining the suitability of a candidate's qualifications, maintaining information on the status of your application;
- to assist us in managing external providers (e.g., recruitment agencies – see below for further information about when we work with third parties);
- to prepare for and enter into a contractual employment relationship.

b) Staff Administration:

- to manage our HR records and update the UBS Group employee database (e.g., keeping your application data on file);
- to communicate with you about any actual or potential job vacancy.

c) Onboarding:

- to set up internal profiles, collecting information required to complete the employee onboarding process. For background checks see d) below);
- to assist us in managing external providers involved in the onboarding process (e.g., insurance companies, pension funds).

d) Compliance & Risk Management and / or Crime Prevention:

- to carry out background checks as part of the employee onboarding process, including checking for any existing or potential conflicts of interest or any other restrictions which may otherwise restrict or prevent a candidate's employment with UBS as well as to prevent crime, including fraud or criminal activity, misuses of our products or services as well as the security of our IT systems, architecture and networks;
- to receive and handle complaints, requests or reports made to a compliance function, HR function, or other designated units within UBS or the UBS Group;
- to reply to any actual or potential proceedings, requests or the inquiries of a public or judicial authority (e.g., if UBS is under a duty to disclose personal data to comply with any legal or regulatory obligation);
- to comply with any legal or regulatory obligations imposed on UBS in relation to its recruitment practices such as governmental reporting requirements.

e) Other purposes:

- to provide information to other UBS Group entities or third parties to benefit from cost-effective services, efficient solutions and subject-matter expertise (e.g., we may opt to use certain IT platforms offered by suppliers. We may also share Personal Data with another UBS entity so that a team with the appropriate subject-matter expertise can provide advice or support);
- to provide information to third parties to enable a transfer, merger or disposal to a potential buyer, transferee, merger partner or seller and their advisers in connection with an actual or potential transfer, merger or disposal of part or all of UBS's business or assets, or any associated rights or interests, or to acquire a business or enter into a merger with it;
- to exercise our duties and/or rights vis-à-vis you or third parties (e.g., if UBS needs to obtain legal advice or provide Personal Data in connection with judicial proceedings);
- to collect data to ensure the security of buildings, as well as property and information located or stored on the premises, and to prevent unauthorized physical access to secure premises (e.g., maintaining building access logs and CCTV system images);
- to create custom and lookalike audiences on various social media platforms allowing to display targeted job advertisements.

We use both automated (including artificial intelligence) and manual methods to process your Personal Data for these purposes. Our automated methods often are related to and supported by our manual methods. For example, our artificial intelligence systems (e.g. Microsoft 365 Copilot) may analyse your data to identify patterns and trends, which are usually manually reviewed and interpreted by humans. Please see section 7.1. for further information on automated decision making.

3.2 Basis for the processing of Personal Data

Depending on the purpose of the processing activity (see section 3.1), the legal basis for the processing of your Personal Data will be one of the following:

- necessary to perform our contractual obligations towards you or to take pre-contractual steps at your request, such as preparing a contract of employment for you following a decision to make you an offer of employment;
- necessary to comply with our legal or regulatory obligations, such as reference requirements;
- necessary for the legitimate interests of UBS, without unduly affecting your interests or fundamental rights and freedoms (see below);
- in some cases, and as may be requested from you from time to time, we have obtained prior consent (such as when we apply automated decision making to evaluate whether to reject or proceed with your application).

Examples of the 'legitimate interests' referred to above are:

- to benefit from cost-effective services, efficient solutions and subject-matter expertise (e.g., we may opt to use certain IT platforms offered by suppliers. We may also share Personal Data with another UBS entity so that a team with the appropriate subject-matter expertise can provide advice or support);
- to determine whether a candidate or potential candidate's skills, qualities and experience are suitable for a role within UBS, and determine whether or not to either (i) make an offer of employment with UBS; or (ii) approach a candidate with a view to making an offer of employment with UBS, on this basis;
- at the appropriate stage in the recruitment process (i.e., as part of making an offer of employment to you), to verify the accuracy of information you have provided to us as part of your application, including through background screening;
- to prevent fraud or criminal activity, misuses of our products or services as well as the security of our intormation, IT systems, architecture and networks and security of UBS premises;
- to create custom and lookalike audiences on various social media platforms allowing to display targeted job advertisements.

You are under no obligation to provide data to us during the recruitment process. However, if you do not provide the information, we may not be able to process your application properly or at all.

4 How do we protect Personal Data?

All UBS employees accessing Personal Data must comply with the internal rules and processes in relation to the processing of Personal Data to protect them and ensure their confidentiality.

UBS and the UBS Group have also implemented adequate technical and organisational measures to protect Personal Data against unauthorised, accidental or unlawful destruction, loss, alteration, misuse, disclosure or access and against all other unlawful forms of processing.

5 Who has access to Personal Data and with whom are they shared?

5.1 Within UBS and the UBS Group

We make available Personal Data to members of our personnel and within the UBS Group for the purposes indicated in section 3.1. Other companies of the UBS Group may process your Personal Data on behalf and upon request of UBS.

5.2 Outside UBS and the UBS Group

For the purposes listed in section 3.1 above, and to the extent permitted under applicable law, we may also transfer Personal Data to third parties outside UBS and the UBS Group, such as:

a) third party service providers, who are contractually bound to confidentiality, such as our IT system or hosting providers, cloud service providers, social media platforms, database providers, consultants (including the recruitment agency whom you used to apply to UBS, if applicable, and lawyers) and third parties who carry out pre-employment checks on prospective employees (such as HireRight);

b) a potential buyer, transferee, merger partner or seller and their advisers in connection with an actual or potential transfer or merger of part or all of UBS's business or assets, or any associated rights or interests, or to acquire a business or enter into a merger with it;

c) authorities, e.g., regulators, enforcement or exchange body or courts or party to proceedings where we are required to disclose information by applicable law or regulation or at their request, or to safeguard our legitimate interests;

d) the referees provided on your application form to UBS;

e) any central or local government department and other statutory or public bodies; and

f) any legitimate recipient of communications required by laws or regulations.

Where UBS or the UBS Group transfer your data to third party service providers processing data on UBS behalf, we take steps to ensure they meet our data security standards, so that your Personal Data remains secure. Third party service providers are thereby mandated to comply with a list of technical and organisational security measures, irrespective of their location, including measures relating to: (i) information security management; (ii) information security risk assessment and (iii) information security measures (e.g., physical controls; logical access controls; malware and hacking protection; data encryption measures; backup and recovery management measures).

5.3 Data Transfers to other countries

The Personal Data transferred within or outside UBS and the UBS Group as set out in sections 5.1 and 5.2, is in some cases also processed in other countries. We only transfer your Personal Data abroad to countries which are considered to provide an adequate level of data protection, or in the absence of such legislation that guarantees adequate protection, based on appropriate safeguards (e.g., standard contractual clauses adopted by the European Commission to the extent recognized by the competent Data Protection Authority or another statutory exemption) provided by local applicable law.

You may request additional information in this respect and obtain a copy of the relevant safeguard by contacting the Group Data Protection Office at dpo-pl@ubs.com.

The transfer of Personal Data to a country which does not grant an adequate level of protection according to the European Commission and/or according to the Monaco Law, or which is not subject to adequate protection, may also subject to a prior authorisation from the relevant Monegasque Data protection Authority.

A list of the countries in which UBS and the UBS Group operates can be found at https://www.ubs.com/global/en/our-firm/locations.html.

6 How long do we store your data?

We will only retain Personal Data for as long as necessary to fulfil the purpose(s) for which it was collected or to comply with legal, regulatory, or internal policy requirements, whichever is longer. In general, although there may be exceptions, data relating to unsuccessful candidates for roles within UBS is kept for 36 months after the date on which we notify you that your most recent application has been unsuccessful; data relating to potential candidates for roles within UBS is kept for 36 months from the date of our last recorded communication with you. Any maximum storage term set forth by applicable local law will prevail. Data relating to successful candidates is dealt with by the employee privacy notice that will be provided to you upon joining UBS. If your application is successful, your application will be retained as part of your personnel record.

However, if you wish to have your Personal Data removed from our databases, you can make a request as described in section 7 below, which we will review as set out therein.

7 What are your rights and how can you exercise them?

7.1 Your rights

You have a right to access and to obtain information regarding your Personal Data that we process. If you believe that any information we hold about you is incorrect, unclear, obsolete or incomplete, you have the right to request the amendment of your Personal Data as appropriate.

You also have the right to:

- object to the processing of your Personal Data, for legitimate reasons;
- request the deletion of your Personal Data if the data is imprecise, incomplete, equivocal, obsolete or if the processing of that data is prohibited;
- request restriction on the processing of your Personal Data; and/or
- withdraw your consent where UBS obtained your consent to process Personal Data (without this withdrawal affecting the lawfulness of any processing that took place prior to the withdrawal).

UBS will honour such requests, withdrawal or objection as required under applicable data protection rules, but these rights are not absolute: they do not always apply and exemptions may be engaged. We will usually, in response to a request, ask you to verify your identity and/or provide information that helps us to better understand your request. If we do not comply with your request, we will explain why.

In certain circumstances UBS may process your Personal Data through automated decision-making. Where this takes place, you will be informed of such automated decision-making that uses your Personal Data and be given information on criteria and procedures applied. Where we do not rely on your prior consent, you can request an explanation about automated decision making carried out and that a natural person reviews the related decision where such a decision is exclusively based on such processing.

7.2 Exercising your rights

To exercise the above rights, please send an email to sh-hr-data-requests-snow@ubs.com.

If you are not satisfied with how UBS processes your Personal Data, please let us know and we will investigate your concern. Please raise any concerns by contacting the Group Data Protection Office at dpo-mc@ubs.com.

If you are not satisfied with UBS's response, you have the right to make a complaint to the Monaco Data Protection Authority (Autorité de Protection des Données Personnelles (APDP)) or in the place where you think an issue in relation to your data has arisen. The contact details of the Data Protection Authority can be found at the following website: https://apdp.mc/.

8 Changes to your Personal Data

We are committed to keeping your Personal Data accurate and up to date. Therefore, if your Personal Data changes, please inform us of the change as soon as possible.

9 Updates to this Notice

This Notice was updated in July 2025. Any amendment or update to this Notice we will make available to you here. Please visit the UBS website frequently to understand the current Notice, as the terms of this Notice are closely related to you.

10 List of UBS employing entities covered by this Notice

Entity Name	Registered Address
UBS (Monaco) S.A.	2 Avenue de Grande-Bretagne, MC98000 Monaco

If you have any questions or comments about this Notice, please contact the Group Data Protection Office at dpo-mc@ubs.com.