

APPLICANT DATA PROTECTION NOTICE: EUROPE

1. INTRODUCTION

This Applicant Data Protection Notice (“**Notice**”) describes the manner by which Sony DADC (“**Company**”) collects, uses, and otherwise processes certain individually identifiable information about applicants (“**Applicant Data**”) in connection with the recruitment relationship. The Company acts as a data controller with respect to the collection, use and other processing of Applicant Data. Please review the Schedule at the end of the Notice for details of the Company applicable to you.

2. CATEGORIES OF APPLICANT DATA WE COLLECT

The Company collects, holds, uses and processes the following categories of Applicant Data:

- > **Personal and family information**, including name, contact information (including home address, telephone and fax numbers and email address), gender, date of birth, photograph (with your consent), nationality and residency information, social security or national insurance number (or other local equivalent), identity card number, passport information (including copies), work permit number (as permitted and required in order to check your right to work), tax identification number(s), government ID, bank account details (for payment and taxation purposes), beneficiaries details (in relation to benefits), emergency contacts, marital status, and information about dependents (where necessary for the provision of applicable benefits, guarantees or crisis management),
- > **Role-related information**, including current and previous job/position titles, company, division, department, supervisor name and title, hire date, seniority date, departure date (where applicable), information regarding qualifications, educational background, work history and previous work experience (including references from previous employers), employment contract information, information regarding expatriated or visa status, work permit and other documentation required under immigration laws, working time and leave entitlements, salary and related compensation data (including bonus information, pay scale area and type and any salary-related changes), military status, and information regarding conflicts of interests (including information contained in conflict of interest certification statements such as any conflicts disclosed).

The Company also collects, processes and uses the following categories of Applicant Data that may be considered “sensitive” under local territory law (“**Sensitive Applicant data**”): physical or mental health conditions where applicable to confer certain special benefits, and, potentially, information regarding an applicant’s unlawful or objectionable behavior.

Where Applicant Data is not listed above (“**Other Data**”), unless the Company requests such specifically, please do not send such Other Data to the Company. Where such Other Data is provided by the applicant to the Company it shall be treated in accordance with the other Applicant Data covered under this notice.

3. PURPOSES OF PROCESSING OF APPLICANT DATA AND LEGAL BASIS

The Company may collect, hold, use and otherwise process Applicant Data for purposes related to your recruitment process, where related to your role, the Company’s business interests and where it is legally required to do so, including, but in no way limited to:

As required to perform the the activities below:

- > facilitating business contacts and communications;
- > recruiting and obtaining references;
- > facilitating emergency contacts; and
- > where permitted by local law and with your consent, conducting background checks to evaluate eligibility for employment.

As required by the Company to enable our business and pursue our legitimate interests, by undertaking the activities below:

- > facilitating management reporting, strategic planning, project management, budgeting, financial management and reporting, risk management, insurance administration, business continuity planning and emergency communications, and recordkeeping;
- > operating and managing information technology and communications systems, including e-mail directories, messaging services and CCTV, access control and other similar systems;
- > protecting the security of applicants, employees, Applicant Data, employee Data as well as safeguarding company systems, assets and premises;
- > conducting audits; and
- > any other purposes related to those listed above.

As required for compliance with applicable laws and protection of the Company's legitimate business interests, by undertaking the activities below:

- > obtaining legal advice;
- > ensuring compliance with legal, regulatory and other requirements as well as company policies and procedures;
- > meeting equal opportunity and anti-discrimination legislation, including gender, race or ethnic origin (where permitted by and in accordance with applicable law);
- > responding to legal process such as subpoenas, pursuing legal rights and remedies, defending litigation; and managing inquiries, complaints, claims or investigations;
- > conducting audits;
- > ensuring compliance with government inspections and other requests from government or public authorities; and
- > facilitating compliance-related training.

The company collects information in training records, hotline reports and conflict of interest certifications for compliance-related purposes, including compliance with legal and regulatory requirements as well as company policies and procedures.

The Company collects, uses and processes Sensitive Personal Data for the following purposes:

- > assessing any special workplace needs or making any necessary adjustments;
- > managing absences;
- > processing and administering benefits and leave entitlements;
- > as applicable, tracking diversity; and
- > complying with legal and regulatory requirements.

When the Company asks Applicants to provide information, we will make clear if Applicants **have** to provide the information to the Company because it is required by law (for example, if the Company has to check a right to work). In these cases, failure to provide mandatory information will affect the Company's ability to employ the Applicant.

If the Company does not say that it is mandatory to provide information, then it is optional to provide the information. However, if Applicants do not provide the Applicant Data that the Company requires for the purposes described above, the Company may not be able to fully provide such Applicants with certain services or benefits.

The Company does not collect, use, disclose, or otherwise process Applicant Data for direct marketing purposes. The Company will retain Personal Data in accordance with its customary HR and employment practices and/or as required by applicable law.

Please note that the Company may retain and process personal data relating to you following your period of employment for purposes of performing administrative tasks related to your employment, and for archival, recordkeeping and legal purposes, in accordance with the Company's customary HR and employment practices, subject to applicable laws.

Sony Corporation of America ("**SCA**"), and Sony Corporation (as defined below in Paragraph V), the Company's other affiliated companies and third parties referred to in Paragraph IV of this Notice may also collect, hold, use, and otherwise process Applicant Data for the fulfilment of all or some of the purposes stated in this Paragraph III and, in particular, in connection with the purposes set out in Paragraphs IV and V, as applicable.

4. DISCLOSURES OF APPLICANT DATA

As part of normal business operations, the Company may disclose Applicant Data to third party service providers in connection with human resources and payroll-related tasks (e.g., banks, insurance companies, travel agents, and other Applicant benefit providers) and for the purpose of operating the Sony Ethics & Compliance Hotline related to compliance with Company policies and procedures and legal and regulatory requirements. The Company may also disclose Applicant Data to third party service providers in connection with information technology support (e.g., software maintenance, remote management of IT infrastructure and applications, development and maintenance of applications, global service desk operations and data hosting) and human resources support (e.g., benefits and human capital management consulting, performance management, talent planning, Applicant training, payroll solutions, and expense reporting). In addition, Applicant Data may also be made available to a third party travel agent which, in turn, may transfer Applicant Data to the Company, its parents and/or affiliates, after the Applicant provides the information to the travel agent.

The Company will (i) exercise appropriate due diligence in the selection of such third party service providers, and (ii) require that such third party service providers maintain adequate technical and organisational security measures to safeguard the Applicant Data, and process the Applicant Data only as instructed by the Company and for no other purposes.

The Company may also disclose Applicant Data to governmental agencies and regulators (e.g., tax authorities), social organisations (e.g., the social security administration), human resources benefits providers (e.g., health insurers), external advisors (e.g., lawyers, accountants, and auditors), courts and other tribunals, and government and quasi-governmental or self-regulatory authorities (including authorities located in the United States, such as the Securities and Exchange Commission or the Department of Justice), to the extent required or permitted by applicable legal obligations.

5. INTERNATIONAL TRANSFERS OF APPLICANT DATA

The Company may transfer Applicant Data to its intermediate parent company SCA in the United States and Sony Corporation in Tokyo, and to any affiliated companies in the US or other territories in connection with certain personnel administration and employment related activities or legal matters. In addition, some of the service providers referred to in Paragraph 4 may be located in other non-local territories. This information is provided as necessary to carry out legal or business obligations, as permitted by this employee consent, as necessary in connection with the performance of contracts, or as otherwise authorised or permitted by applicable law.

The Company has ensured that personal data transferred to SCA in the US and any potential transfers onward to Sony Corporation are protected in accordance with the Standard Contractual Clauses adopted by the European Commission. You may obtain a copy by contacting DADCEUROPELEGAL@sonydadc.com.

In accordance with applicable laws, the Company may monitor your e-mail for legitimate business purposes, including compliance with company policies, procedures and applicable U.S. law.

6. ACCESS TO APPLICANT DATA

Applicants generally have the right to access, review, update, correct and request the deletion or restriction of their own Applicant Data in accordance with applicable law. You may also ask us to transfer some information that you have provided us to another organisation. For example, where we have processed data based on your consent, you have a right to withdraw that consent, and where we rely on legitimate interests, you have a right to ask us not to do this. These rights may be limited in some situations. For example it may not affect data we have already collected with your consent, or we may have a legal requirement to still process your data. Additionally, subject to applicable laws, the Company may also retain information in its original form and/or delay correcting information until any related dispute as to the applicable information is resolved. Also, applicants are responsible for informing the Company if there are any changes or inaccuracies to their Applicant Data. Applicants should transmit any requests for access, transfer or updates to, or corrections or deletions or restrictions of their own Applicant Data to the Company in writing as specified below in Paragraph 7.

7. QUESTIONS ABOUT PROCESSING OF APPLICANT DATA

Applicants who have any questions about this Notice or wish to (i) access, transfer, review, correct or request the deletion or restriction of their Applicant Data or learn more about who has access to such information, or (ii) report a concern related to Applicant Data, should contact PRIVACY@sonydadc.com and/or DADCEUROPELEGAL@sonydadc.com. If you have unresolved concerns, you also have the right to complain to data protection authorities.

8. SECURITY PRACTICES AND PROCEDURES

The Company has adopted reasonable security practices in compliance with applicable law to secure the Applicant Data. This includes, amongst other measures, the adoption of the Sony Global Information Security Policy & Standards (“GISP & GISS”).

.....

Sony DADC

Please remember that any personal data that you process as an applicant of the Company must be in accordance with applicable laws and our Data Protection Policy.

SCHEDULE

| |
|---|
| Sony DADC Europe Limited |
| Sony DADC Europe Limited, Zweigniederlassung Österreich |
| Sony DADC Germany GmbH |
| Sony DADC France SAS |
| Sony DADC Czech Republic s.r.o |
| Sony DADC Iberia SL |
| ENS Entertainment Network Scandinavia AB |
| OOO Sony DADC (Russia) |
| Sony DADC Hong Kong Limited |
| Sony DADC China Co. Limited |
| Shanghai Epic Music Entertainment Co. Limited |
| Sony DADC Manufacturing (India) Private Limited |
| Sony DADC Australia Pty. Limited |

Please note that we may revise this Schedule from time to time to reflect changes in our corporate structure.