|  |
| --- |
| **Transfer Impact Assessment Vendor Questionnaire** |

|  |  |  |
| --- | --- | --- |
|  | *Will your company (“data importer”, “you” or “your”) process personal data of NICE or NICE’s customers?* | Yes  No |

The following questions are required to be answered if your company processes personal data of NICE or NICE’s customers.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vendor Details** | | | | |
|  | *What does your company do?*  *Provide details of the products or services you will provide to NICE.* | [Give details] | | |
|  | *Is your company a telephone, email, or internet service provider (ISPs) or remote computing service provider that provides “computer storage or processing services” to the public?* |  | | |
|  | *Why will you process the personal data?*  *Please explain what processing activities you will perform.* | [Give details] | | |
|  | *Will you sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing or by electronic or other means, any personal data, or inferences related thereto, to another business or a third party for monetary or other valuable consideration?* |  | | |
|  | *Where (in what country or countries) will you process personal data in order to provide products and services to NICE?* | [Give details] | | |
|  | *Can the processing be conducted solely in the European Economic Area (EEA) (for EEA personal data) or UK (for UK personal data)? For example, is a dedicated EEA service team offered as an accommodation?* | [Give details] | | |
|  | *Have you conducted a data protection impact assessment ("DPIA") for this processing (or similar processing), or assisted other customers in relation to a DPIA for this kind of processing to date?* | Yes, and we can provide you with a copy of this DPIA.  Yes, however, we cannot provide you with a copy of this DPIA.  No | | |
|  | *Will you onward transfer the personal data to other third parties? If so, please complete the table to identify (i) all such third parties and their location; (ii) why they will receive and/or process the personal data; and (iii) where they will process the personal data.*  Note: Both "transfer" and “onward transfer" include remote access. Onward transfer can be to the same or another third country. | Yes  No  If yes, please provide details below: | | |
| **Third party recipient details (including name and location)** | **Why will it process the personal data?** | **Where will it process the personal data?** |
|  |  |  |
|  |  |  |
|  |  |  |
|  | *If there are onward transfers to other third parties, please confirm whether you have performed due diligence on such third parties on substantially similar terms or better than those in this questionnaire, whether Transfer Impact Assessments have been carried out in each case and if you are able to provide us with copies of these Transfer Impact Assessments?* | Yes, due diligence has been performed on substantially similar terms or better than those in this questionnaire, TIAs have been conducted and are available at [give details / annexed to this questionnaire].  No, due diligence has not been performed on substantially similar terms or better than those in this questionnaire or TIAs have not been conducted because [give details]. | | |
|  | *Will your company process personal data outside of the EEA, UK or a jurisdiction subject to an adequacy decision by the European Commission?* | Yes  No | | |

The following questions are required to be answered if personal data will be processed by you outside of the EEA, UK or a jurisdiction subject to an adequacy decision by the European Commission. The EC has previously recognized Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom and Uruguay as adequate, but you are responsible to confirm such determinations are current.

|  |  |  |
| --- | --- | --- |
| **Personal Data** | | |
|  | *Will your services require the processing of personal data that easily identifies the data subjects? For example, will the data directly identify the individual by name and address or official ID number (passport, social security, etc)? Or will the data be fully anonymised by aggregation or pseudonymised (including by encryption) and the key remains protected in the EEA/UK?* |  |
|  | *Will your services require the processing of communications data or metadata, including but not limited to internet communication activity, telephone records, electronic communication archive and history?* |  |
|  | *Will your services require the processing of special category data (including biometric data), criminal offence-related data, or can such data be inferred from the data transferred?*  Note: “special category data” includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation. |  |
|  | *Will your services require the processing of financial data?* |  |
| **Access to personal data by public authorities** | | |
|  | *Have you implemented a government data access policy that governs your response to a request to access or disclose data to a government agency?* | [Give details, if applicable] |
|  | *Can you confirm whether you have or have not received requests for access to personal data from public authorities in the past and that you are not prohibited from providing information about such requests or their absence?* | Yes, we can confirm we have received [e.g. 1-250] requests [in the past year/other time period] and are not prohibited from providing information about such requests or their absence.  No, we are prohibited by law from providing this information. |
|  | *Can you confirm whether you or your permitted subprocessors are or have been subject to requests pursuant to Section 702 of the US Foreign Intelligence Surveillance Act (FISA), “Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons” (50 U.S.C. sec. 1881a).* | Yes  No |
|  | *Please provide an overview of any laws granting public authorities in the jurisdictions where you process personal data the right of access to data or requiring disclosure of personal data (for instance, for criminal law enforcement, regulatory supervision or national security purposes) held by Company or accessible/processed by third parties.* |  |
|  | *Please provide an overview, to the extent known to counsel, of any evidence that the authorities in the jurisdictions where you process personal data seek to access data held by you or via third parties without your knowledge (considering reported legal precedents, legislation and practice).* |  |
|  | *Please provide an overview, to the extent known to counsel, of any elements demonstrating that an authority in the jurisdictions where you process personal data will be able to access data held by you, for example through direct interception of a communication channel, considering reported precedents, legal powers, and technical and human resources at the authority’s disposal.* |  |
|  | *Is the law/practice in the jurisdictions where you process personal data based on clear, precise and accessible (publicly available) rules?* |  |
|  | *If a public authority seeks to exercise powers under the applicable law/practice in the jurisdictions where you process personal data, is it required to justify that its actions are necessary to meet its objective / purpose?* |  |
|  | *Is there an independent and impartial oversight mechanism in relation to the exercise of the powers under the applicable law/practice? Please confirm whether this oversight mechanism is subject to public scrutiny.* |  |
|  | *Do individual data subjects in the jurisdictions where you process personal data have the right and ability to receive redress and remedy where the applicable law/practice impacts or prevents the exercise of their rights under applicable law?* |  |
|  | *Do foreign data subjects (data subjects who are not considered a citizen of the jurisdictions where you process personal data) have the same rights of redress and remedy to those of citizens?* |  |
| **Identify the additional safeguards taken to protect the transferred personal data** | | |
| **Technical measures** | | |
|  | ***Encryption in transit:*** *Is the personal data encrypted end-to-end with state of the art, robust encryption while transiting third countries without essentially-equivalent protection on its way to you in a country whose public authorities can access personal data in transit?*  Note: “Essentially equivalent” here refers to countries that are subject to an adequacy decision by the European Commission. The EC has previously recognized Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom and Uruguay as adequate, but you are responsible to confirm such determinations are current. | Yes  No  If Yes, will the encryption key remain protected in the EEA/UK or a jurisdiction offering essentially equivalent protection?  Yes  No |
|  | ***Encryption at rest:*** *Is the personal data encrypted while transiting third countries without essentially-equivalent protection on its way to you in a country whose public authorities can access personal data at rest?* | Yes  No |
|  | ***Transfer with access to personal data in the clear:*** *Will the data be accessible in cleartext (i.e. non-encrypted) ?* | Yes  No  Please give details: [Give details] |
|  | ***Pseudonymisation:*** *Will the data be pseudonymised prior to transit to third countries?*  Note: “Pseudonymisation” means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. | Yes  No  Please give details: [Give details] |
|  | *Have you implemented any other technical measures to protect the privacy of the personal data? Tick any of the following that apply.* | The data importer uses privacy enhancing technologies such as secure multi-party computation ("MPC") or homomorphic encryption, to protect the privacy of personal data.  [Give details] |
| **Organisational measures** | | |
|  | *Does your organisation have any internal policies, organisational methods, and/or standards in relation to personal data transfers and access requests?* | Please tick all that apply.  Adequate internal policies exist with clear allocation of responsibilities for personal data transfers, reporting channels and standard operating procedures for formal or informal requests to access the data (especially for intragroup transfers), including appointment of a specific team (IT, data protection and privacy experts) to deal with requests that involve personal data transferred from the EEA; notification to senior legal and corporate management and to the data exporter upon receipt of such requests; procedural steps to challenge disproportionate or unlawful requests; and provision of transparent information to data subjects.  Training is in place for personnel in charge of managing requests for access, periodically updated to reflect new legal developments in the importing territory and EEA, including on EU requirements as to access by public authorities to personal data, in particular Article 52 (1) Charter of Fundamental Rights, raising awareness of personnel by assessment of practical examples of public authorities’ data access requests and by applying the Article 52(1) standard to the practical examples, taking into account data importer territory legislation and regulations applicable to the data importer (developed where possible in cooperation with the data exporter).  [Give details] |
|  | *Are there transparency and accountability measures regarding public authorities' access to personal data?* | Tick the following if applicable.  The data importer documents and records requests and responses provided to access requests, including legal reasoning and actors involved; and these will be made available to the data exporter.  [Give details] |
|  | *Do you implement confidentiality, audit and escalation measures governing transfers of, and access to, personal data?* | Tick any of the following that apply.  The data importer has in place strict and granular data access and confidentiality policies and best practices, based on a strict need-to-know principle, monitored with regular audits and enforced through disciplinary measures, focusing on data minimisation with technical measures to restrict access (it might not be necessary to transfer certain data e.g. restricting remote access to EEA data for support, or when service provision only requires transfer of a limited dataset and not the entire database).  Development of best practices to appropriately and timely involve and provide access to information to the data protection officer, if any, and to legal and internal auditing services on matters related to international transfers of personal data, before the transfer is effected.  [Give details] |
|  | *Can you evidence the adoption of standards and best practices?* | Tick the following if applicable.  The data importer has in place strict data security and data privacy policies, based on EU certification or codes of conducts or on international standards (e.g. ISO norms) and best practices (e.g. ENISA) with due regard to the state of the art, in accordance with the risk of the categories of personal data processed.  [Give details] |
|  | *Have you implemented any other organizational measures to protect the privacy of the personal data? Tick any of the following that apply.* | The data importer has adopted and regularly reviews internal policies to assess suitability of implemented complementary measures and identify and implement additional or alternative solutions when necessary, to ensure that an essentially equivalent level of protection is maintained.  The data importer has provided commitments not to engage in any onward transfer of the personal data within the same or other third countries, or suspend ongoing transfers, when an essentially equivalent level of protection cannot be guaranteed.  [Give details] |

**Vendor Details**

|  |  |
| --- | --- |
| Vendor Full Legal Name |  |
| Contact person’s name, position, and contact details |  |
| Date |  |