| | | |
|---|---|---|
| Project Title | : | OverTTuRe - Italy |
| Application Name | : | OverTTuRe - Italy |
| Status | : | Reviewed - Risk Mitigation Acceptable |
| Reviewer | : | OMISSIS |
| Author | : | OMISSIS |
| SET Area | : | BioPharmaceuticals |
| AZ System/ Service Owner | : | OMISSIS |
| Estimated date (month/year) in which the solution is rolled out | : | December 2025 |
| Confidential PIA? | : | OMISSIS |
| Sign-Off Date | : | 04/03/2026 13:59 UTC |
| Risk Assessment | : | OMISSIS |

## Threshold

## Overview

1. Please provide a brief overview of the project/system/application in simple, non-technical terms, including how Personal Data will be used to support the project/system/application. For guidance as to what personal data is, *the guidance document on personal data here.* If you have any documents that would help describe the system/process/application, please note that these can be uploaded in the last TAB of the PIA ("Submission").

OverTTuRe Italy is an observational, cohort study sponsored by AstraZeneca AB, which will include patients with a confirmed diagnosis of transthyretin amyloidosis (ATTR) with the aim of providing an Italian perspective in the pre- and post-diagnosis disease journeys, including baseline characteristics, treatment patterns and selected clinical, economic and humanistic outcomes. This study will include data from patients aged at least 18 years old and will use secondary data extracted from medical records. Data will be registered into an electronic CRF by the study personnel after confirmation of the inclusion criteria for the study. OMISSIS

Subjects will be involved in the study, provided that they meet the study eligibility criteria and provided approval for their data inclusion in the study is obtained from the Independent Ethics Committees (IECs). Living subjects will be involved in the study after signature of ICF&PF, according to Italian Data Protection Regulation. Deceased and untraceable subjects could be involved in the study pursuant to art. 110 of the Italia Privacy law, Guidelines issued on 9th May 2024 by the Italian Data Protection Authority and Regole Deontologiche per la ricerca statistica e scientifica.

2. Please describe the PURPOSE for using personal data as part of this project/system/tool. Where the purpose is linked to AZ´s legitimate business interests/needs, please describe what those interests/needs are

The legal basis for collecting and processing personal data depends on the subject:

1) PATIENTS (Study Participants). The legal basis is the patient's consent (art. 6.1a) and art. 9.2 a) GDPR). AZ will collect consent from study participants for taking part in the study (Informed Consent Form) and processing of personal data (Data Privacy Consent Form), both of which are needed for the subject to participate in the study. Such consent will be collected according to relevant laws, regulations, standards, and internal AZ procedures.
Deceased and untraceable subjects could be involved in the study pursuant to art. 110 of the Italia Privacy law, Guidelines issued on 9th May 2024 by the Italian Data Protection Authority and Regole Deontologiche per la ricerca statistica e scientifica. Legal basis in this case is art. 9.2 j) and par. 4, art. 36 and 89 GDPR in addition art. 110.1 d.lgs. 196/2003. The inclusion of deceased or untraceable subjects is crucial to minimize risk of selection bias, as defined in Protocol.

2) HCPs (Study Staff). The legal basis is a legal obligation, since AZ needs to collect certain basic data about study sites' staff involved in the conduction of a clinical study in order to comply with regulatory requirements.

3) THIRD PARTIES (External Service Provider: CRO). The legal basis is a legitimate interest of AZ in processing data of the CRO staff in order to ensure delivery of all activities in which the CRO has been engaged according to the executed service agreement.

| | | |
|---|---|---|
| 1. | Does the solution process (i.e. collect, store, share or otherwise use) personal data? which can directly or indirectly identify a living person? E.g. Name, PRID, IP address, email, E-code etc. Further guidance as to what constitutes personal data can be found in the guidance document on personal data *here*. | Yes |
| 2. | Does the solution only process the following basic low risk employee personal data: name, business contact details or PRID? | No |
| 3. | Does the business activity system or project collect, store, process or use any of the following categories of sensitive personal data?<br><br>Physical or mental health or condition<br>Race or ethnic origin<br>Political opinions<br>Religious or other similar beliefs<br>Trade Union membership<br>Sexual life<br>Genetic data<br>Biometrics data (such as iris scans, fingerprints, facial recognition)<br>Commission, or alleged commission, of any offence or proceedings relating to an offence.<br>Financial information other than basic transactional data such as bank accounts to support making contractual payments or managing employee expenses. (Financial information that is used for more than making payments should be treated as sensitive personal data. This may include information relating to an individual's assets or debts, their spending habits or patterns or credit score.)<br>Official identification numbers (such as passport or social security numbers)<br>Locational Information (Track Info, precise positioning info (GPS), residential address info, Geo Fencing etc.) | Yes |

| | | |
|---|---|---|
| 4. | Will the business activity collect, collect, store, process or use a high volume of personal data?<br><br>When answering this question please see the guidance below on what amounts to a high volume of personal data.<br><br>HR Personal Data<br>(Regional or Global) - personal data records relating to more than 7000 employees/candidates/contractors HR Persona Data<br>(Country) - personal data records relating to more than 10% of employees/candidates/contractors in the specific country.<br>HCP Personal Data<br>(Regional or Global Initiative)- more than 100,000 HCP's personal data record HCP Personal Data.<br>(Country) - personal data records relating to more than 10% of the HCPs in that specific country.<br>Patient Data - More than 1000 patient personal data records. | No |
| 5. | Is this a local, global or multiple initiative? | Local |
| 6. | Will the business activity use personal data for the purpose of profiling, automatic decision making or will it utilise innovative and new technology.<br><br>You should only answer yes to this question if the business activity will do any of the following:<br><br>Use personal information to produce an automated score or evaluation of individuals including assessing their behaviours or predicting how they may behave in the future<br>Use personal information to make a fully automated decision, without any meaningful human review or input, that will have a legal or similarly significant impact on an individual.<br>Combining existing data sets to create a new data set relating to individuals<br>Using new technology that has not generally been used for similar purposes by either AstraZeneca or a similar organisation. | No |
| 7. | Does the solution involve the use of CCTV cameras or other similar systems that systematically monitor areas? | No |
| 8. | If this initiative relates to an IT system/application, has this system been registered in Service Now (for internal systems) or the Digital Asset Inventory (for external facing websites, mobile apps and social media sites)? | Not Applicable |
| 9. | Will the business activity use personal data relating to vulnerable individuals e.g. , patients or people with health conditions, employees, children, asylum seekers, the elderly, other than basic personal data for a legitimate reason i.e.: name and basic contact details or basic employee information to allow for system access such a PRID or email address? | Yes |
| 10. | Could the business activity use personal data to prevent individuals using a service, entering into a contract or exercising their rights? | No |

| | | |
|---|---|---|
| 11. | Have you attended a PIA Clinic with a member of the Privacy Office when completing this PIA? | No |
| 12. | Does the business activity or project encompass the development, acquisition or use of any Artificial Intelligence (AI)* capabilities? | No |

## Personal Data

| | | |
|---|---|---|
| 1. | Does your project utilise personal data related to employees or employee candidates?<br>Please select all the applicable personal data types.<br>- Name<br>- Business contact details (business address, telephone number, mail address). | Yes |
| 2. | Does your project utilize personal data related to patients or children (under 16 years OR under 14 in China) participating in AZ's clinical trials, pharmacovigilance activities, patient centricity programs etc?<br>Please select all the applicable personal data types.<br>- Patient eCode<br>- Personal Characteristics (gender, age, nationality, languages spoken)<br>- Family (facts about family members)<br>- Health (current and past physical and mental health condition or status); Height, weight, BMI, etc.<br>- Genetic (genetic characteristics – DNA and related analysis) | Yes |
| 3. | Does your project utilise personal data related to patient carers or patient support people? | No |
| 4. | Does your project utilise personal data related to Healthcare Professionals (HCPs)?<br>Please select all the applicable personal data types.<br>- Name<br>- Business contact details (business address, telephone number, email address)<br>- Employment related (general employment details such as job description, CV, work history, qualifications, etc)<br>- Certificates and licenses (professional certification etc) | Yes |

| | | |
|---|---|---|
| 5. | Does your project utilise personal data related to other third parties (i.e. other than HCPs)? Examples of third parties are AZ's suppliers, service providers, consultants, collaboration partners etc.<br>Please select all the applicable personal data types.<br>- Name<br>- Business contact details (business address, telephone number, mail address)<br>- Personal financial information (personal financial accounts and credit)<br>- Certificates and licences (professional certification etc) | Yes |
| 6. | Does your project utilise personal data about children (under 16 years OR under 14 in China)? | No |
| 7. | Can any of the personal data be classified as sensitive personal data?<br>Please select all the applicable personal data types.<br>- Physical or mental health condition<br>- Genetic Data<br>- Pseudonomised and de-identified health data | Yes |
| 8. | Is all personal data strictly required to achieve the purpose of your project? Before answering, please read the guidance on the right hand side. | All Personal Data Required |
| 9. | Does this project involve any new uses of personal data that is already held by AZ (e.g. the use of the data for a new purpose) OR can the personal data potentially be misused, to make decisions or inferences about Data Subjects? e.g. unauthorized surveillance of employee activities. Please specify what those new uses are or the likelihood of misuse and mitigating controls applied | No |
| 10. | Will the personal data being utilized be de-identified at any point in the process? | No |

## Scope

| | | |
|---|---|---|
| 1. | Where will the project/system/application be utilised? | Local |
| 2. | Where are the data subjects located (i.e. where do they reside)? | Local |

| | | |
|---|---|---|
| 3. | Where are the users of the system or application that collects, stores, shares or uses the personal data located? | Local |
| 4. | Please select the country location(s) where the system or application will be hosted, backed up in (or located for Disaster Recovery purposes). If more than 1 system is being utilised in the process please attach the IT architecture blueprint as evidence.<br><br>A cross-border data transfer self-assessment must be completed when personal data of individuals based in China is accessed or transferred between AZ legal entities in China, AZ legal entities outside China or to/by a Third Party outside of China. Please contact our Chinese Deputy Data Protection Officer listed OMISSIS for support completing the assessment. | |
| 5. | | |

## Third Parties & Partners

| | | |
|---|---|---|
| 1. | Has AstraZeneca contracted with a third party to use a third party technology OR third-party processing services as part of this project, process or system? | Yes |
| 2. | Please provide the following information about the third party/parties engaged/contracted by AstraZeneca:the legal names of the third party/parties specify for each third party whether they have access to personal data or whether the third party stores personal data<br>a brief description of how the third party/parties will have access to or store the personal data, including how personal data will be used to support the process, project or system | Yes |
| | Third party: OMISSIS. This vendor will be responsible for this project (EC submission, sites contracting, eCRF development & maintenance, data capture, data management, and data analysis & reporting). OMISSIS Italy will process pseudo-anonymized personal data through eCRF/EDC. The data will be analysed according to Study Protocol and Statistical Analysis Plan in order to provide publication and study report. An access is limited to those personnel working on this specific project. | |

| | | |
|---|---|---|
| | Third party: OMISSIS. This vendor will be responsible for this project (EC submission, sites contracting, eCRF development & maintenance, data capture, data management, and data analysis & reporting). OMISSIS Italy will process pseudo-anonymized personal data through eCRF/EDC. The data will be analysed according to Study Protocol and Statistical Analysis Plan in order to provide publication and study report. An access is limited to those personnel working on this specific project. | |
| | If you are obtaining personal data from third parties, have you ensured that the third parties have a lawful basis to collect and/or share the personal data in the first place? | Yes |
| 3. | Have you ensured that the third party(ies) have gone through appropriate data privacy due diligence processes as part of AZ's Third Party Risk Management Process? (Nb. More information about due diligence can be found OMISSIS) | Yes |
| | Please provide the Engagement Number for the Third Party Risk Management process. For AZ engagements you can check all existing 3PRM assessments OMISSIS<br><br>OMISSIS | |
| 4. | Have you ensured that the contracts with these third parties contain appropriate data protection terms? (Nb. Templates with language for contracts can be found OMISSIS) | Yes |
| | Please attach a copy of the data privacy clauses which will cover the processing of personal data by the 3rd party. This may be part of contractual documentation and may include agreement schedule, appendices or EU Model Clauses which have been signed. For existing Vendors, appropriate terms may have already been signed (check the existing contractual documentation and attach a copy).<br><br>*Please do not attach anything else than excerpt/s from your full contract documentation covering the data protection clauses and the contact information about the parties to the agreement in order to avoid sharing any information that may be of sensitive commercial nature to both AstraZeneca and/or the third party, which should be kept confidential.*<br><br>Fully executed contract is attached. | |

| | | |
|---|---|---|
| 5. | A Transfer Impact Assessment (TIA) must be completed when EU EEA/UK Personal Data is <u>transferred</u> to/and or being <u>accessed</u> by a Third Party. <br><br>The TIA can be accessed at the following link OMISSIS | Yes |

## Notice & Consent

| | | |
|---|---|---|
| | Is there a current Privacy Notice that covers the uses of the personal data? | |
| 1. | A key principle of privacy legislation is that we have to be transparent about what personal data we are collecting, how we use it, who we share it with and how data subjects can exercise their legal rights of access, rectification and deletion. This is usually done through a Privacy Notice which is provided to the data subject at the time we start collecting their Personal Data. Failure to implement a Privacy Notice is a breach of data privacy law. | Yes |

If you are using one of AZ standard Privacy Notices, these are stored in AZ master repository for Privacy Notices and can be accessed through the following link for AZ OMISSIS. Please copy the link to the relevant Privacy Notice and paste it into the free text box below. Please note that if a third party is publishing an AZ standard Privacy Notice on our behalf (e.g. on their own on-line mobile app or website) you need to ensure that said third party displays the relevant link to the Privacy Notice in AZ's master repository referred to above. This is important to ensure that the latest version is always made available to the data subjects.<br><br> If you are using a bespoke AZ Privacy Notice or a third-party Privacy Notice, please upload a copy for review.

Informed Consent Form and data privacy notice will be provided to patients that are alive at the time of enrolment. For deceased/untraceable patients, the privacy notice will be published on the company website. An adopted ICF attached.

If you are using one of AZ standard Privacy Notices, these are stored in AZ master repository for Privacy Notices and can be accessed through the following link for AZ OMISSIS. Please copy the link to the relevant Privacy Notice and paste it into the free text box below. Please note that if a third party is publishing an AZ standard Privacy Notice on our behalf (e.g. on their own on-line mobile app or website) you need to ensure that said third party displays the relevant link to the Privacy Notice in AZ's master repository referred to above. This is important to ensure that the latest version is always made available to the data subjects.<br><br> If you are using a bespoke AZ Privacy Notice or a third-party Privacy Notice, please upload a copy for review.

Informed Consent Form and data privacy notice will be provided to patients that are alive at the time of enrolment. For deceased/untraceable patients, the privacy notice will be published on the company website. An adopted ICF attached.

Are you relying on Consent as the legal basis for processing personal data?

2. In some countries you must obtain Consent from the data subjects before processing their personal data. Most countries with privacy legislation will require Consent for processing Sensitive Personal Data. Failure to obtain Consent where this is required is a breach of data privacy law. Yes

Please note however that to rely on Consent when processing personal data is often regarded as a less favorable option, as it can be withdrawn at any time. Furthermore, it shall never be used when an employer is processing personal data about its employees as it would not be deemed as freely given.Please note that the Consent referred to above is not the same as the "Informed Consent" required to enroll patients into clinical studies.

Informed Consent Form and data privacy notice will be provided to patients that are alive at the time of enrolment. For deceased/untraceable patients, the privacy notice will be published on the company website. AZ ICF template for an observational study is attached.

Please note however that to rely on Consent when processing personal data is often regarded as a less favorable option, as it can be withdrawn at any time. Furthermore, it shall never be used when an employer is processing personal data about its employees as it would not be deemed as freely given.Please note that the Consent referred to above is not the same as the "Informed Consent" required to enroll patients into clinical studies.

Informed Consent Form and data privacy notice will be provided to patients that are alive at the time of enrolment. For deceased/untraceable patients, the privacy notice will be published on the company website. AZ ICF template for an observational study is attached.

## Personal Data Lifecycle & System Security

| | | |
|---|---|---|
| 1. | Are there any other process, project or system that interface, extract or consume personal data in or out of this system? | Yes |
| | Please explain the processes, projects or systems that interface with this one and how? Please attach a document detailing the flows of personal data between systems, including the location and method of transfer e.g. Secure File Transfer Path (SFPT); encrypted email etc. If applicable please provided PIA number of the processes, projects or systems.<br>Data from eCRF / EDC will be sent to AZ repository -OMISSIS | |
| 2. | Access to personal data should only be granted to people with a strict need to know. Please confirm how you comply with this requirement by stating the people including any third parties or external individuals that will be given access to personal data and why. | |

This requirement is stated in study documents as Study Protocol. Observational study data will be stored in a computer database, maintaining confidentiality in accordance with local laws for Data Protection. In case source data verification will be planned as quality check, Monitor of company representing AZ may require direct access to source documents that are part of the hospital or practice records relevant to the observational study. All eCRF user roles are defined according to the level of access needed (Data Management Plan) and the user access will be given according to the requests received from the Clinical Research Associate or site staff. Only people who have a clear business need to have access to Personal Data are granted access.
Patients' pseudonymized personal data will be collected into the eCRF. Access to such eCRF will be possible only with personal accounts after login (username and password). Such accounts will only be granted to CRO study staff who signed a confidentiality agreement, works under the privacy clauses of the Service Agreement between AZ and the CRO, and has a genuine need to access the system (eg. CRAs, data managers).
Site Study staff can only access to the patients' eCRF of their site. Same access measures are in place. Patients' personal data will also be stored in the Investigator Site File [ISF] as per current regulations and standards of clinical research; the ISF is paper-based and it is only accessible by study staff at the study site and CRAs (for the purpose of monitoring activities, as required by current standards for clinical research and detailed in a Monitoring Plan). At the conclusion of the Study, the data will be transferred by CRO to the Study Sites and to Sponsor through validated secure web-systems which apply security measures such as data encryption and multifactor authentication. Access will be granted only to authorized person. The Final Study Report will contain aggregated data and will be reviewed only by AZ employees who have a legitimate role. Personal data of study staff (HCPs and CRO staff) will be only processed by people involved in the study within either AZ and the CRO.

| | | |
|---|---|---|
| 3. | Has IT Security Governance carried out an IT Security Assessment of the process, project or system? An IT Security Assessment is a high-level cyber security review of IT solutions, services and Third Parties. The aim of the assessment is to protect AstraZeneca through the identification of potential risks, providing recommendations and agreeing risk treatment options to comply with AstraZeneca policies and standards. You can request an IT Security Assessment OMISSIS. | Yes |

Please provide the Ticket Number for the IT Security Assessment (please also ensure to attach a copy of the same as evidence in the last tab)

OMISSIS

| | |
|---|---|
| Will all recommendations made by Information Security be actioned? | Yes |

| | | |
|---|---|---|
| 4. | Has a time frame been established for how long the initiative retains personal data? OMISSIS | Yes |
| | Please provide the number of years that you aim to retain the personal data and if applicable, the GRAD reference number. | |
| | 5 years OMISSIS | |
| | Have you determined a process to delete personal data once the retention time has passed? | Yes |
| 5. | Please provide details in the space below of how you have assured that the personal data being processed is accurate and will be kept up-to-date. If the personal data is taken from an existing master data set held by AstraZeneca please name the source e.g. Workday, Veeva etc | Yes |
| | During the study the CRO (OMISSIS) representative implements different activities to assure compliance with AZ standards of quality.<br><br>Contacts with the sites to:<br>• Provide information and support to the healthcare professionals and other site personnel.<br>• Confirm that the research team is complying with the protocol and that data are being accurately recorded in the CRFs.<br>• Ensure that the CRFs are completed properly and with adequate quality. Monitoring activities for checking that patients exist in medical records (a sample).<br><br>A study monitoring plan, including for-cause monitoring, that is appropriate for the study design will be developed and implemented. Clinical Research Associates will perform Source Data Verification (SDV) according to the Monitoring Plan and will validate data entry procedures in terms of accuracy and consistency regarding source documents. All data validations involving range checks, time differences, logical checks and data consistency within the eCRF are the responsibility of the Clinical Data Manager.<br><br>All data validation checks are documented. These specifications are defined during study setup and are intended to ensure that all collected data is checked for inconsistencies, in order to guarantee its maximum quality. | |
| 6. | Will personal data be held in any development or test environment? | No |

## Risk & Remediation

***Due Diligence***

RISK: No risks found.

***Contractual Clauses***

RISK: No risks found.

***Transparency : Notice and Consent***

RISK: No risks found.

***Data Minimization / Proportionality***

RISK: No risks found.

***Access controls***

RISK:
Access controls may not be sufficient/appropriate (e.g. people who do not have a clear business need to have access to Personal Data are provided access).
REMEDIATION:
Please review your access controls to ensure that only people who have a clear business need to have access to Personal Data are granted access.

| | |
|---|---|
| Above risk has been identified. Will it be re-mediated? If risk is not applicable, please select no and explain why. | Yes |
| User Comments: | |
| Access will be limited by both parties to those individuals with an assigned role in the study; only for the purpose to conduct the study according to the study protocol and statistical analysis plan. All people involved in the project activities will have signed a Confidentiality Agreement. Data protection terms have been established within the executed Service Agreement signed between AZ and OMISSIS(CRO). Patients' personal data will be and remain pseudonymised at all times thus minimising the risks associated with any breaches. Access to eCRF will be possible only with personal accounts, and such accounts will only be granted to study staff who signed a confidentiality agreement, works under the privacy clause of the Service Agreement between AZ and the CRO, and has a genuine need to access the system (eg. CRAs, data managers). Patients' personal data will also be stored in the Investigator Site File [ISF], as per current regulations and standards of clinical research; the ISF is paper-based and it is only accessible by study staff at the study site and CRAs (for the purpose of monitoring activities, as required by current standards for clinical research and detailed in a Monitoring Plan). Personal data of study staff (HCPs and CRO staff) will be only processed by people involved in the study within either AZ and the CRO. Data stored in Sponsor or Sponsor representatives system have safeguards in place to prevent any unauthorised access. | |

***Security***

RISK: No risks found.

***Retention***

RISK: No risks found.

***Works Council***

RISK:
Because the right to protect an individuals´ personal space and personal information is a fundamental right, when processing personal data about employees or prospective employees, in some countries you may need to consult with the Works Councils due to labor law requirements. Situations where this may apply are in relation to activities that involve any type of employee monitoring (such as installation of CCTV cameras, system monitoring to validate compliance with internal policies, etc.) or any type of profiling activities. Collecting or sharing "sensitive data" about employees (unless legally required) or transferring employee data to "non adequate countries" (i.e. countries that have not been confirmed by the European Commission to have an adequate level of data protection laws). may also require notification to the Works Council.

The handling of basic low risk employee personal data (employee name, business contact details or PRID) should NOT trigger the need to consult with Works Councils.

Please *consult with HR* as to how to proceed.

| | |
|---|---|
| Above risk has been identified. Will it be re-mediated? If risk is not applicable, please select no and explain why. | No |
| User Comments: | |
| Not applicable as only basic employee data is processed as part of this activity to enable individuals to perform their duties. | |

***Third Parties and International Transfers***

RISK:
A number of countries have prohibitions on transferring Personal Data outside the country of origin/region. This includes the storage of, and / or access to, personal data by a third party (AstraZeneca has measures in place to legitimize transfers between AZ entities).For any transfers of personal data to third parties, you should consider whether the third party has access to personal data via a terminal (e.g. a computer screen) or whether the third party provides hosting services. If the access or hosting by the third party is outside the EEA, you should put in place Model Contract Clauses with the third party (note: these may already be in place if it is a third party that has been engaged by AZ before). Your Procurement partner can assist with this task. If you do not have support from Procurement, you can find Model Contract Clauses by clicking on the *data privacy clauses* link. Alternatively, AZ can rely on consent of individuals to legitimize an international transfer of personal data.

| | |
|---|---|
| Above risk has been identified. Will it be re-mediated? If risk is not applicable, please select no and explain why. | Yes |
| User Comments: | |
| TIA completed. OMISSIS. | |

***Privacy Network***

RISK: No risks found.

## Further Supporting Evidence

| | | |
|---|---|---|
| 1. | Please confirm that the technology (internal or external) utilised in the project, process or system described within this PIA, has been implemented in accordance with our Privacy by Design Standard. OMISSIS. | Not Applicable |

## Review

***Notification to Authorities***

**Is notification to the Data Protection Supervisory Authority Required?**

Occasionally, AstraZeneca's EU Privacy Rep may be required to notify data protection authorities of the outcome of a PIA. Below "decision tree" is intended to assist Privacy Reps when determining whether it is appropriate to inform their regulatory authority following a PIA and to make such deliberation easier and more consistent across the company. For additional information and extensive guidelines please *click here* or contact the *Privacy Office*.

| | | |
|---|---|---|
| 1. | Does this PIA involve processing of personal data from EU/EEA data subjects? | |

*Outcome/Recommendation :*

No need to inform the Data Protection Supervisory Authority

## Status

Status : Reviewed - Risk Mitigation Acceptable

Comments:
Please update consent form

| | |
|---|---|
| Does the PIA require notification to the Privacy Network? | No |
| Please confirm who the Controller or Controllers are for this processing system/activity. For more information see the links *All AZ Entites Globlally* and *All AZ Entities in the EEA* | All AZ Entities in the EEA |