URIM APP LIMITED - DATA PROTECTION POLICY

PURPOSE

This document sets out URIM's prevailing Data Protection Policy, to ensure conformance with relevant current UK legislation, including **UK-GDPR**. UK-GDPR replaces EU GDPR. Its purpose is to protect the "rights & freedoms" of natural persons (ie living individuals), to ensure that personal data is not processed without their knowledge and, wherever possible, their consent. This document should be read in conjunction with the maintained versions of the separate documents: "URIM Information Security & Business Continuity Policy" (IS&BCP).

OBJECTIVES

This Policy is intended to:

1. Be capable of implementation and enforceable under URIM's BMS & specifically under the existing IS&BCP.
2. Be appropriately concise & easy enough to be understood by all relevant Stakeholders (Staff, Partners, Clients, Auditors, etc).
3. Balance essential data protection with necessary operational productivity
4. Fulfil its Purpose as outlined above
5. Facilitate and ensure adherence to UK-GDPR, EU-USA 'Standard Contractual Clauses' legal provisions and other prevailing legislation, as well as conformance to Contractual Service expectations, specified by individual Clients.

DEFINITIONS

1. **Personal Data**: Any information relating to an identified, or identifiable natural person ('data subject'); an identifiable natural person being one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
2. **Special Categories of Personal Data**: 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.

DATA PROTECTION PRINCIPLES

1. This Data Protection Policy operates under the auspices of URIM's wider prevailing "Information Security & Business Continuity Policy" and its associated BMS (encompassing its Objectives & Principles).
2. It goes into greater Policy detail regarding Customer Data as a sub-category of "Information", specifically including "Personal Data" and "PII", as referenced under **UK-GDPR**.
3. URIM holds PII as a Data Processor, on behalf of its Clients. It also may hold PII as a Data Sub-Processor on behalf of certain Business partners, as a sub-contractor.
4. URIM does not knowingly hold any Special Categories of PII (such as ethnicity, banking information, blood type, etc) as defined under GDPR & above. However, the Content of each URIM Client Instance is managed and controlled directly by the URIM Customer themselves, for which they are accountable.
5. All Personal Data held or processed by URIM, will be processed fairly & lawfully.

6. URIM will ensure that for all Personal Data it holds, the relevant Data Controller is known and the purpose for which the Data will be processed is known & shared, specifically to: “Permit communications with the associated natural persons via the listed Contact Devices, in the context of operational events and/or emergencies, plus associated operational exercises”.
7. Consent, obtained by the Data Controller, must & will be revocable, via the authenticated request of the Natural Person, via support@URIMapp.com , using the relevant Natural Person’s originating email address as listed, or via URIM’s designated authorised Contact(s) for the relevant Service Contract.
8. URIM will maintain a Data Privacy Breach Process as follows:
    a. Identification of when a Data Privacy breach occurs, notified via email to support@URIMapp.com , via the relevant automated process (eg SIEM or other monitoring process), or individual/organisation identifying the relevant Breach.
    b. Responding to the Data Privacy Breach in accordance with the prevailing Incident Management Process, capturing all relevant collateral information (hardware, software, documentation, logs, as preservation of evidence) to assist with diagnostics and root cause analysis & alerting the relevant Stakeholders, including the Client & the ICO. Such evidence to be allocated under the direct control of the CEO/CISO, or their designated immediate deputy for the task.
    c. Engagement of the relevant subject matter expertise (eg forensic cyber security analysis) within the organisation & outside it as required, to assist in timely recovery from & resolution of the relevant Breach.
    d. Formal Review (“Key Meeting” format) & Publication of an associated Data Breach Report, including assessment of the implications of the breach, following issue resolution, to all relevant Stakeholders.
9. URIM will maintain an Information & Revocation Process, upon authorised request, via Support@URIMapp.com , whereby:
    a. The initial request for either Information (held), or Revocation (requested) is acknowledged by reply to that initial request, within 24 hours
    b. The processing of that request is achieved within 72 hours of the initial request
    c. The “Closure” email confirmation will be sent back to the originating email mailbox, as an audit trail.
    d. All such requests will be audited & reviewed by URIM DPO at least monthly.
    e. Any issues arising with the above process can be emailed direct to URIM’s DPO via ceo@urim.app .
10. Client Data (including all Personal Data from Clients & Business Partners) is given the highest Information Security Classification within URIM (“Secret”), on a par with URIM’s own Company Intellectual Property.
11. All Client Data (as opposed to Data about clients/customers) shall be sourced directly from Clients (via authorised and Contractually designated Client representatives and/or processes), with Clients being required to verify and authenticate that, as the relevant Data Controller, they have obtained & maintain the proper opted-in permissions and suitable supporting policies & processes, under UK-GDPR.
12. URIM will provide suitable support to Clients (Data Controllers) by discharging its duties as a Data Processor, including the appropriate monitoring and control of its own Data Sub-Processors.
13. URIM will provide suitable support to its Business Partners by discharging its duties appropriately as a Data Sub-Processor.
14. URIM will only receive and hold the minimum amount of Client Data sufficient to perform its Contractual Services, associated with the provision of Operational

Notifications, to Client Staff and other designated Contacts. All Client Data will be used only for the purposes intended by the Data Controller (the Client or Business Partner, as detailed within the relevant Contract) and will only be held for the minimum period required to discharge its associated Service delivery responsibilities (by default, for the period of associated Contract Duration, plus a minimum reasonable period thereafter, to technically execute the removal of the Client Data from associated URIM systems – but in no cases to exceed 72 hours after the end of the Contract period).

15. URIM will ensure the proper safeguarding and protection of Client Data while in its care, whether as Data Processor or Data Sub-Processor. URIM will use industry good practice guidelines, in applying "Privacy Enhancing Technologies" (PETs) to help protect Client Data under management. Clients should content themselves that such detailed provisions are adequate for their needs, according to the Client's own Data Protection Risk Assessments, or otherwise notify URIM, under relevant Contract variation and notification clauses, allowing URIM reasonable time to remedy any perceived shortcomings. In the unlikely event that any shortcomings cannot be remedied, URIM will (upon request) provide the Client with an electronic (eg CSV/XLS) digital Data Extract of the relevant Client Data (Contacts), prior to ultimate removal from URIM systems, such that the Client can provide that Data Extract to an alternate Service Provider, as necessary.
16. URIM will maintain a map of where Personal Data is held. Unless otherwise stated, this will be within separate logical Client instances of MySQL Server databases, held on virtual servers, in UK 'Tier 3' data centres. All sites and Personal Data instances, are thus held within the UK.
17. URIM will maintain logical separation between Development, Test & Production environments. Client Personal Data will only be held in Production environments. URIM will maintain appropriate separation of duties between Development, Administration, Security & Support staff & functions.
18. **Privacy Policy & Privacy Notices**: URIM neither gathers, nor holds data about natural persons, without their express consent. It does not capture web visitor information, nor does it use 'Cookies'. It only holds minimal technical details (originating device IP address) sufficient to maintain a current web session with the connected device, for the duration of the session (Note: In many cases, IP addresses will be dynamically applied by the local country ISP & URIM does not correlate the resulting IP address information with other information sources, to identify probable country/location of IP address origin). URIM systems do not gather/hold Personal Data beyond the Data that authorised Client System users, or associated Business Partners (Data Processors), supply and/or enter themselves.
19. All Clients (or their Data Processors), as ultimate Data Controllers, are required to evidence that they have obtained the necessary permissions of the relevant natural persons (members of Client staff and other designated Contacts, under the relevant Service Contract), to hold the relevant Personal Data, passed to URIM.

DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

1. DPIA is a process to help URIM identify and minimise the Data Protection risks of its operations.
2. URIM will conduct a DPIA for any type of processing that is likely to result in a high risk to Client Data. URIM uses the DPIA screening checklist below, as recommended by the UK ICO.

3. DPIA's will:
    a. Describe the nature, scope, context & purpose of the processing. The purpose will always be in order to provide the Contractual Services required by the Client as the Data Controller, or by the Business Partner as the Data Processor – and for no other reasons.
    b. Assess the necessity, proportionality & compliance measures.
    c. Identify & assess risks to individuals
    d. Identify any measures to mitigate those risks.
4. In assessing the level of risk, URIM will assess both the likelihood and severity of the impact on individuals, identifiable by PII, within the Client Data (ie High Risk of some harm, or Low Risk of serious harm).
5. URIM's DPO will consult the relevant subject matter experts as required.
6. If URIM identifies a High Risk that it cannot mitigate, it will contact the ICO before conducting any processing & will adhere to the ICO's guidance & timelines in the matter.
7. CHECKLISTS:
    a. DPIA Awareness Checklist
        i. We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.
        ii. Our existing policies, processes and procedures include references to DPIA requirements.
        iii. We understand the types of processing that require a DPIA, and use the screening checklist to identify the need for a DPIA where necessary.
        iv. We have created and documented a DPIA process.
        v. We provide training for relevant staff on how to carry out a DPIA.
    b. DPIA Screening Checklist
        i. We always carry out a DPIA if we plan to:
            1. Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
            2. Process special category data or criminal offence data on a large scale.
            3. Systematically monitor a publicly accessible place on a large scale.
            4. Use new technologies.
            5. Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
            6. Carry out profiling on a large scale.
            7. Process biometric or genetic data.
            8. Combine, compare or match data from multiple sources.
            9. Process personal data without providing a privacy notice directly to the individual.
            10. Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
            11. Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
            12. Process personal data which could result in a risk of physical harm in the event of a security breach.
        ii. We consider carrying out a DPIA if we plan to carry out any other:
            1. Evaluation or scoring.
            2. Automated decision-making with significant effects.

3. Systematic monitoring.
4. Processing of sensitive data or data of a highly personal nature.
5. Processing on a large scale.
6. Processing of data concerning vulnerable data subjects.
7. Innovative technological or organisational solutions.
8. Processing involving preventing data subjects from exercising a right or using a service or contract.
9. If we decide not to carry out a DPIA, we document our reasons.

iii. We consider carrying out a DPIA in any major project involving the use of personal data.
iv. We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

c. **DPIA Process Checklist**

i. We describe the nature, scope, context and purposes of the processing (relevant for responding to DSARs).
ii. We ask our data processors to help us understand and document their processing activities and identify any associated risks.
iii. We consider how best to consult individuals (or their representatives) and other relevant stakeholders.
iv. We ask for the advice of our data protection officer.
v. We check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure data protection compliance.
vi. We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.
vii. We identify measures we can put in place to eliminate or reduce high risks.
viii. We record the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.
ix. We implement the measures identified, and integrate them into our OPERATIONAL & project plans.
x. We consult the ICO before processing if we cannot mitigate high risks. We keep our DPIAs under review and revisit them if necessary.

8. **DEFAULT DPIA FOR ALL URIM CLIENTS:**

a. In this DPIA:

i. The nature, scope, context & purpose of the processing is as follows. To enable URIM to provide the Contractual Services required by the Client as the Data Controller, (or by other Business Partners as the Data Processor) – and for no other reasons (Scope). The Contractual Services are to provide: "Digital Communications with the target information Recipients via the URIM System, with authorised URIM User account contact details." (Nature, context & purpose).
ii. Assesses the necessity, proportionality & compliance measures. The existing policies and measures governing Client Data are deemed sufficient, as detailed in the prevailing versions of the following documents:
    1. URIM Information Security & Business Continuity Policy
    2. "How Does URIM safeguard My Data?"
    3. This Data Protection Policy
iii. Identifies & assess risks to individuals

There is risk of loss of data, corruption of data, or data breach. In the event of a data breach, the individual's contact details could be made known and abused, with the consequent impact of nuisance & potential impersonation. Incorrect or lost data could materially impact the ability of a Client organisation to contact its members of Staff (or other listed Contacts) in the event of emergency, with potential impact of personal harm, or even loss of life.

iv. Identifies any measures to mitigate those risks.
The risks are mitigated by ensuring a high degree of confidence in data integrity, availability and security. Impacts of individual device detail errors are minimised, by assisting clients to ensure data is suitably checked and device contact details are verified during scheduled testing exercises & rehearsals.

b. In assessing the level of risk, URIM has assessed both the likelihood and severity of the impact on individuals, identifiable by PII, within the Client Data (ie High Risk of some harm, or Low Risk of serious harm).
c. URIM's DPO will continue to consult the relevant subject matter experts as required, for any matters extending beyond existing arrangements (eg evolving cyber security threats over time).
d. If URIM identifies a High Risk that it cannot mitigate, it will contact the ICO before conducting any processing & will adhere to the ICO's guidance & timelines in the matter. No High Risks were identified. Currently, all Risks for Data held within URIM systems are assessed as Low. NB: Clients are responsible for the accuracy (or otherwise) of the Client Data supplied.
e. DPIA Awareness Checklist
    i. We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.
    ii. Our existing policies, processes and procedures include references to DPIA requirements.
    iii. We understand the types of processing that require a DPIA, and use the screening checklist to identify the need for a DPIA where necessary.
    iv. We have created and documented a DPIA process.
    v. We provide training for relevant staff on how to carry out a DPIA.
f. DPIA Screening Checklist
    i. We have carried out a DPIA for Client Data within URIM, as per the following Checklist:
        1. Use systematic and extensive profiling or automated decision-making to make significant decisions about people. NO.
        2. Process special category data or criminal offence data on a large scale. NO.
        3. Systematically monitor a publicly accessible place on a large scale. NO.
        4. Use new technologies. YES
        5. Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit. NO.
        6. Carry out profiling on a large scale. NO.
        7. Process biometric or genetic data. NO.
        8. Combine, compare or match data from multiple sources. NO.
        9. Process personal data without providing a privacy notice directly to the individual. YES.

10. Process personal data in a way which involves tracking individuals' online or offline location or behaviour. YES. (Tracking authorised User activity once logged into the system, via System Logs).
11. Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them. NO.
12. Process personal data which could result in a risk of physical harm in the event of a security breach. YES. (If Contact Data became corrupted, or lost & the Individual was not adequately contacted in an actual emergency, wherein there was direct risk of harm).

ii. We will carry out a further DPIA if we plan to carry out any other:
1. Evaluation or scoring.
2. Automated decision-making with significant effects.
3. Systematic monitoring.
4. Processing of sensitive data or data of a highly personal nature.
5. Processing on a large scale.
6. Processing of data concerning vulnerable data subjects.
7. Innovative technological or organisational solutions.
8. Processing involving preventing data subjects from exercising a right or using a service or contract.
9. If we decide not to carry out a DPIA, we document our reasons.

iii. We will consider carrying out a DPIA in any major project involving the use of personal data. (Use within URIM App already qualifies).
iv. We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

g. **DPIA Process Checklist**
i. We describe the nature, scope, context and purposes of the processing. YES.
ii. We ask our data processors to help us understand and document their processing activities and identify any associated risks. YES.
iii. We consider how best to consult individuals (or their representatives) and other relevant stakeholders. YES.
iv. We ask for the advice of our data protection officer. YES.
v. We check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure data protection compliance. YES.
vi. We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests. YES.
vii. We identify measures we can put in place to eliminate or reduce high risks. YES.
viii. We record the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted. YES. The outcome of this DPIA on [12/01/21] is that the existing measures continue to be fit for purpose, in satisfying both UK-GDPR & Client requirements, as well as industry good practice guidelines.
ix. We implement the measures identified, and integrate them into our Operational & Project plans. YES.
x. We consult the ICO before processing if we cannot mitigate high risks. YES (does not apply for this DPIA).

xi. We keep our DPIAs under review and revisit them if necessary. YES (at least every 6 months, as part of the Company Review, under ISO22301 & ISO 9001 compliance audits.

DSAR PROCESS

1. The DSAR can be received via any valid communications method into the URIM organisation, or its staff, from valid Data Controllers.
2. Such valid DSARs are captured, documented & forwarded to support@urimapp.com where they are assessed & reviewed for operational validity. DSARs are then processed using a specific database search (on the unique Username/email of the data subject), with the output generated as a PDF &/or Excel output file, for sharing with the Data Controller.
3. All such valid DSARs are forwarded to ceo@urimapp.com to be reviewed & managed, for onward supply to the Data Controller by the CEO, with associated electronic audit trial, through to closure of the DSAR case.
4. All DSARs are reviewed as part of the monthly Operational Review Process.

ROLES AND RESPONSIBILITIES

1. This document is owned by the CEO, who is also URIM's DPO & CISO.
2. All URIM staff are individually responsible for adhering to URIM's prevailing applicable policies and procedures, relevant to information security & data protection, relevant to their own respective roles & responsibilities.
3. Functional Heads are each responsible through their line management, for ensuring adherence to this Policy within their Functional Area.
4. All Staff will each complete an annual Information Security online training test, via "IT Governance", (or similar system as notified by their line manager), as part of their responsibility to maintain their own Information Security awareness levels, within role.
5. Clients (via designated Contractual Contacts) are responsible:
    a. For providing URIM with evidence of Consent from natural persons listed as Contacts within the Client Data; and
    b. For maintaining timely Contact/Device Detail accuracy & integrity in the Client Data provided, under their own Duty of Care to their Staff/Contacts.

CHANGE CONTROL

1.0	01/04/19	Initial Version
2.0	12/01/21	Updated for UK-GDPR & SCC's