# Data Protection Policy

| Policy information | |
|---|---|
| **Organisation** | Urban Stream Ltd |
| **Scope of policy** | Applicable to all Urban Stream Ltd entities and activities including all EU operations.<br><br>3rd Parties may also process data in accordance with GDPR. |
| **Policy operational date** | 16/3/21 |
| **Policy prepared by** | Dale Taylor |
| **Date approved by Board/ Management Committee** | 16/3/24 |
| **Policy review date** | 16/3/24 |

| Introduction | |
|---|---|
| **Purpose of policy** | • Compliance with GDPR<br>• Protection of that of our staff, clients and individual's data<br>• Good practice to ensure we are safeguarding data we hold or process |
| **Types of data** | No special category data of that identified under article 6 and/or 9 will be processed.<br><br>Types of data processed include:<br>• Web usage data<br>• Web metadata<br>• Email data<br>• Data required for that of billing and order processing<br><br>Data not processed but held securely include:<br>• Client cloud data storage |
| **Policy statement** | Urban Stream Ltd shall:<br>• comply with both the law and good practice<br>• respect individuals' rights<br>• be open and honest with individuals whose data is held<br>• provide training and support for staff who handle personal data, so that they can act confidently and consistently<br>• Notify the Information Commissioner voluntarily, even if this is not required |
| **Key risks** | • Email and web usage data (including user metadata) is stored for a period of 7 years in compliance with Investigatory Powers Act 2016 applying to data service providers<br>• This data carries risk as it could identify individuals and may contain confidential material<br>• Banking information is also stored by our 3rd party suppliers where customers pay by direct debit and/or credit card<br>• This data carries risk as this information could be utilised to commit fraud<br>• Call Data Records and Call Recordings are stored by our 3rd party supplier<br>• This data carries risk as the information could be utilised to commit fraud |

| Responsibilities | |
|---|---|
| **The Board / Company Directors** | Dale Taylor (CEO) |
| **Data Protection Officer** | Dale Taylor (CEO)<br><br>Responsibilities include:<br>• Briefing the Board on Data Protection responsibilities<br>• Reviewing Data Protection and related policies<br>• Advising other staff on tricky Data Protection issues<br>• Ensuring that Data Protection induction and training takes place<br>• Notification to the ICO<br>• Handling subject access requests<br>• Approving unusual or controversial disclosures of personal data<br>• Approving contracts with Data Processors |
| **Employees** | All staff are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. (From now on, where 'employees' is used, this includes both paid employees and volunteers.) |
| **Enforcement** | Training on data protection is given to all staff to ensure compliance with data protection policies. We implement the use of online training providers to ensure our staff remain up to date with latest legislation and training is regularly reviewed.<br>Where we fail to meet the standards set out in this policy the staff member will be retrained to ensure they understand the data protection policies. Multiple or serious violations may result in dismissal and legal action against said individual. |

| Security | |
|---|---|
| **Scope** | How we secure our data including our business continuity planning. This is applicable to all Urban Stream Ltd entities. |
| **Setting security levels** | C1 – Company Classified<br>C2 – Company Secure<br>C3 – Shared under NDA and controlled<br>C4 – Publicly available |
| **Security measures** | C1 – Password protected document that must not leave Urban Stream Network controlled equipment, with list of data holders that must be kept<br><br>C2 – Password protected document that must be stored on Urban Stream Network controlled equipment or on Data Iron hardware encrypted data storage<br><br>C3 – Password protected document<br><br>C4 – No measures required<br><br>Urban Stream operates a clear desk policy with strict access to network equipment and offices.<br><br>Password policies are in place to ensure that data is kept secure at all times and passwords are changed on a regular basis.<br><br>We operate using latest NIST approved encryption operating a minimum 256bit key system.<br><br>Hardware encryption is utilised on all equipment that is connected over the Internet. |
| **Business continuity** | Urban Stream operates an N+1 cloud-based network resilience such that should our main operations centre fail we have the ability to fail over to a secondary site and restore operations in a timely manner.<br><br>Our telecoms operations are fully redundant using latest cloud service providers that offer multiple location resilience. |
| **Specific risks** | Staff do work from home at Urban Stream but we provide a secure encrypted hosted environment in which our staff can operate securely from home without risk of data leakage.<br><br>Our mail services offer protection from "phishing" and we do regularly test to ensure our staff are aware of scams such as this. |

| Data recording and storage | |
|---|---|
| **Accuracy** | We try to maintain accurate information where possible<br>We do regularly check the data we have from our customers including billing information and email addresses. This is particularly important when we have received this information over the phone. |
| **Updating** | We do review all the data we hold on our systems on a regular basis. Where data should not be held such as CV's these are removed. |
| **Storage** | All Urban Stream data is stored in cloud based encrypted storage systems. Full auditing of the storage is available through the solution we utilise such that we can ensure the data is used correctly.<br><br>Our data provider secures our storage using NIST approved encryption systems. |
| **Retention periods** | CV Data – 6 Month<br>Data classified under Investigatory Powers Act 2016 – 7 Year<br>Financial Data required for HMRC – 5 Year |
| **Archiving** | All data related to network activities and delivery of ISP services is archived using online tools from that of our service partners. This data is stored in online secure storage as per the Investigatory Powers Act 2016.<br><br>Other none ISP related data will be disposed of when no longer required or the retention period has expired using secure data deletion tools. |

| Right of Access | |
|---|---|
| **Responsibility** | The data controller is responsible for ensuring that individuals data can be accessed under rights of access within 1 month as per GDPR. |
| **Procedure for making request** | Right of access requests must be in writing. This must be emailed to support@urbanstream.co.uk with the title "Data Access Request". |
| **Provision for verifying identity** | Individuals identity will need to be verified in order to process an access request this can include but is not limited to:<br><br>- Copy of photo ID to be provided<br>- Proof of address in order to mail the requested data |
| **Charging** | A charge of £10 may be levied in order to process the subject access request. |
| **Procedure for granting access** | Where the data is provided electronically this will be provided in common "Microsoft" or "Adobe" formats. |

| Transparency | |
|---|---|
| **Commitment** | Urban Stream processes data for the following purpose:<br>• Run and operate and internet service provider as governed under UK law<br>• Run and operate a telecommunications service as governed under UK law<br>• Effectively bill our customers for services rendered<br>• Provide IT support to our customers<br>• Improve our service to our customers<br><br>Foreseen disclosure events:<br>• Call data records and/or call recordings where data is required as evidence<br>• Email and/or web metadata where data is required as evidence<br>• Data governed by Investigatory Powers Act 2016 cannot be removed or modified by a subject<br>• All other data may be amended or removed at request |
| **Procedure** | Data subjects can find the latest information on our policies through the following channels:<br>• the handbook for employees<br>• on the web site |
| **Responsibility** | We are all responsible for securing our data and that of our customers; we each have a clear defined responsibility. This should be at the forefront of our minds when we work with our customers. |

| Lawful Basis | |
|---|---|
| **Underlying principles** | Data is stored for the following purposes:<br>• Provision of Internet Services<br>• Provision of Telecommunications Services<br>• Delivering remote management services to our customers<br>• Providing simple mechanisms to interact with us |
| **Opting out** | Where data is held outside of the requirements of that of HMRC and/or Investigatory Powers Act 2016 people may opt out of storing and processing their data. To opt-out please email our support teams at support@urbanstream.co.uk |
| **Withdrawing consent** | Once a user has opted out no further data outside of that required by law will be processed for or on that individual. This is not retrospective and previous data may still be stored in accordance with law. |

| Employee training & Acceptance of responsibilities | |
|---|---|
| **Induction** | Employees shall undergo data protection training as per the induction process within Urban Stream. |
| **Continuing training** | Online refreshers on data protection are conducted every 18 months to ensure our staff are kept abreast of latest developments. |
| **Procedure for staff signifying acceptance of policy** | The data protection policy and guidelines are within staff handbook and are part of the contract of employment to ensure that our staff understand the importance of data within our organisation. |

| Policy review | |
|---|---|
| **Responsibility** | Next policy review will be conducted by Dale Taylor. |
| **Procedure** | The review will be managed as a cross functional team reviewing data and usage across the company. |
| **Timing** | The review is expected to take 2 months and will commence 4 months before the next policy update is required. |

For more information, please visit the ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/