The Planet eStream Unified Video Platform and GDPR Compliance

This document is intended to provide a summary of useful information pertaining to the EU General Data Protection Regulation with particular reference to users of the Planet eStream Unified Video Platform (UVP), whether the eStream software suite is hosted by the licensed organisation on their own infrastructure, or on a Planet eStream cloud service platform. The information provided should enable organisations to have confidence that that they can provide access to their Planet eStream resource in full compliance with GDPR obligations.

Disclaimer

This content is provided for informational purposes only and should not be relied upon as legal advice, or to determine how GDPR might apply to any individual organisation. The information is provided “as-is" and Planet eStream makes no warranties (express, implied or statutory) as to the content included in this document.

What Is the GDPR?

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonise data privacy laws across Europe, to protect and empower the data privacy of all EU citizens and to reshape the way organisations across the region approach data privacy.

When Does the GDPR Take Effect?

The GDPR takes effect on May 25, 2018. The GDPR actually became law in April 2016, but given the significant changes some organisations will need to make to align with the regulation, a two-year transition period was included.

Who Does the GDPR Apply To?

The GDPR applies to **‘controllers’** and **‘processors’**

A **controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

A **processor** means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

Where Does the GDPR Apply?

The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

What Information Does the GDPR Apply To?

The GDPR applies to ‘**personal data**’ meaning any information relating to an identifiable natural person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. This data is often referred to as PII (Personally Identifiable Information).

The GDPR also refers to '**sensitive personal data**' as "special categories of personal data" (see Article 9).
Special category data is more sensitive, and so needs more protection. For example, information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

Principles

The GDPR is underpinned by six data protection principles, which set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that:
"The controller shall be responsible for, and be able to demonstrate, compliance with the principles"

Lawful Basis for Processing

Organisations must have a valid lawful basis in order to process personal data. There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the purpose and relationship with the individual.

The individual's right to be informed under Article 13 and 14 requires people to be provided with information about your lawful basis for processing. This means these details need to be included in a privacy notice.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

- Consent: the data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- Contract: processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

- Legal Obligation: processing is necessary for compliance with a legal obligation to which the controller is subject.

- Vital Interests: processing is necessary in order to protect the vital interests of the data subject or of another natural person.

- Public Task: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

- Legitimate Interests: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (This can not apply if you are a public authority processing data to perform your official tasks).

Which Lawful Basis Is Applicable?

The type or organisation processing the personal data is very relevant to determining the lawful basis that applies. Under the current designations of Public Authorities, many educational establishments are included in this classification. Schedule 1 of the Freedom of Information Act (FOIA) sets out the bodies or holders of office that are public authorities under FOIA in the following broad categories:

- Government departments, legislative bodies, and the armed forces.
- Local government.
- National Health Service.
- **Maintained schools and further and higher education institutions.**
- Police.
- Other public bodies (this includes a list of individually named non-departmental public bodies).
- **Academies** that were brought into the FOI regime by the Academies Act 2010.

If you are a **Public Authority** and can demonstrate that the processing is to perform your tasks as set down in UK law, then you are able to use the **public task** basis. If not, you may still be able to consider consent or legitimate interests in some cases, depending on the nature of the processing and your relationship with the individual. There is no absolute ban on public authorities using consent or legitimate interests as their lawful basis, but the GDPR does restrict public authorities' use of these two bases. For example, a University or School might rely on public task for processing personal data for teaching and research purposes; but a mixture of legitimate interests and consent for alumni relations and fundraising purposes. Other organisations may typically designate legitimate interest, contract or consent as the appropriate lawful basis for processing PII.

Individual Rights

The GDPR aims to give individuals more control over the ways in which their Personal Data is processed.
The GDPR provides the following rights for individuals:

The Right to Be Informed

Data subjects must be provided with various information about the data processing activities you carry out.

- This information is usually provided in a Privacy Notice or Privacy Statement.

The information must be:

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge.

The Right of Access

You must provide data subjects with:

- Confirmation their data is being processed;
- Access to their personal data; and
- Other supplementary information, which largely corresponds to the information that should be provided in a privacy notice (see Article 15).

- You must comply with any subject access request within one month of receipt.
- You cannot charge a fee unless the request is "manifestly unfounded or excessive".
- Where you process a large quantity of information you can ask the data subject to specify the information they want access to.
- You may refuse to comply with a subject access request where this is "manifestly unfounded or excessive".

The Right to Rectification

Data subjects can have their personal data rectified if it is inaccurate or incomplete.

- You must comply with any request to rectify within one month of receipt. This can be extended to 2 months where the request is complex.
- Where you are not taking action in response to a request for rectification, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

The Right to Erasure

The right to erasure is also known as 'the right to be forgotten'. Data subjects have the right for their data to be erased where:

- The personal data is no longer necessary in relation to the purpose for which it was collected/processed;
- The data subject withdraws their consent or objects to the processing and there are no overriding legitimate interest to continue processing;
- The personal data was unlawfully processed or has to be erased in order to comply with a legal obligation; or
- The personal data is processed in relation to the offer of information society services to a child.

You can refuse to erase a data subject's personal data where it is processed:

- To exercise a right of freedom of expression and information;
- To comply with a legal obligation or for the performance of a task of public interest;
- For the exercise or defense of legal claims; or
- For purposes relating to public health, archiving in the public interest, scientific/historic research or statistics.

If you have disclosed the personal data to third parties then you must inform them about the erasure of the personal data.

The Right to Restrict Processing

Data subjects have the right to restrict the processing of personal data where:

- They have contested its accuracy;
- They have objected to the processing and you are considering whether you have a legitimate ground which overrides this;
- Processing is unlawful and the individual opposes erasure and requests restriction instead;
- You no longer need the data but the data subject requires it to establish, exercise or defend a legal claim.

If you have disclosed the personal data to third parties you must inform them of the restriction on the processing of the personal data, unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individuals about these recipients.

You must inform individuals when you decide to lift a restriction on processing.

The Right to Restrict Processing

The right to data portability allows data subjects to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

The right to data portability only applies:

- To personal data a data subject has provided to a controller;
- Where the processing is based on consent or the performance of a contract; and
- Where processing is carried on by automated means.
- You must provide the personal data in a structured, commonly used and machine readable form (e.g. CSV or XML files).

- If the individual requests it, you may be required to transmit the data directly to another organisation if this is technically feasible. However, you are not required to adopt or maintain processing systems that are technically compatible with other organisations.
- You must comply with the data subject's request free of charge and within one month. This can be extended to 2 months where the request is complex or if you receive a number of requests.
- Where you are not taking action in response to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

The Right to Object

Data subjects have the right to object to:

- Processing based on legitimate interests, the performance of a task in the public interest or the exercise of official authority (including profiling);
- Direct marketing (including profiling); and
- Processing for scientific/historic research or statistics.

- You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.
- Where the data subject objects to direct marketing you must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.
- Where a data subject otherwise objects to you processing their personal data then you must comply with this request unless you can demonstrate overriding compelling legitimate grounds to continue processing or that the processing is for the establishment, exercise or defence of legal claims.

Rights in Relation to Automated Decision Making and Profiling.

Data subjects have the right not to be subject to a decision when:

- It is based on automated processing; and
- It produces a legal effect or a similarly significant effect on the individual.

You must ensure data subjects are able to:

- Obtain human intervention;
- Express their point of view; and
- Obtain an explanation of the decision and challenge it.

"Profiling" is any form of automated processing intended to evaluate certain personal aspects of a data subject, in particular to analyse or predict their performance at work, economic situation, health, personal preferences, reliability, behaviour and location.

The above right does not apply if the automated decision:

- Is necessary for entering into or performance of a contract between you and the individual;
- Is authorised by law (e.g. for the purposes of fraud or tax evasion prevention);
- Is based on explicit consent; or
- Does not have a legal or similarly significant effect on the data subject.

When processing personal data for profiling purposes, you must ensure that appropriate safeguards are in place.

For example:

- Being fair and transparent about the logic involved;
- Using appropriate mathematical/statistical procedures;
- Implementing appropriate technical and organisational measures to correct inaccuracies and minimise the risk of errors; and
- Keeping personal data secure in a proportionate way.

As a general rule, it is best to avoid making automated decisions based on sensitive personal data unless you have the explicit consent of the data subject or have reasons of substantial public interest.

The ICO provide a **privacy notes code of practice** document at
https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

Personal Data Breaches

1) In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2) The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3) The notification referred to in paragraph 1 shall at least:
   a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   c) describe the likely consequences of the personal data breach;
   d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4) Where, and insofar as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5) The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

The Lead Supervisory Authority (LSA) for the UK is the Information Commissioner's Office (ICO).

Planet eStream UVP Support for Data Controllers

In line with the overview and general principles of the GDPR summarised above, data controllers will need to be aware of how any personal data is data is stored and processed in conjunction with the use of a range of software applications, including the Planet eStream UVP.

Planet eStream is developed in line with the principals of 'Privacy by Design' and 'Privacy by Default'.
A limited amount of personalised data is retained in the Planet eStream databases and is stored and processed appropriately in line with the overall design, feature sets and intended operation of the system.

Data Management

The Planet eStream software suite includes various features which can assist data controllers in complying with obligations imposed by the GDPR. These include:

Access Control

Granular controls over the scope of data access by users are core features of the Planet eStream UVP. The abilities to retrieve and view media, edit existing media and metadata, add new media and gain access to administrative tools are all controlled by schema configurations managed by the data controller.

Content Management

Tools are included in the Planet eStream product to help administrators manage their media content. Particular examples are the 'Content List' and 'Batch Edit' tools and the 'Statistics Module' features.

Feature Review

The Planet eStream UVP is subject a continuous programme of system and feature development. Additional features which may provide further assistance to data controllers are currently under review.

Enhanced features to assist data controllers to ensure GDPR compliance include:

- A 'Disclaimer' notice option, enabling an organisation's administrators to present a suitable policy statement which users can be required to accept before uploading any media content to the system.

- Additional options to present 'Privacy' and 'Consent' related notices to users accessing the system, including acceptance confirmation logging.

- Additional asset 'Ownership' options to enable 'Pseudonymisation' / 'Anonymisation' of personally identifiable data records relating to asset tagging, statistics and analysis. This may be desirable in terms of an organisation's data retention policies, or in response to valid requests for the removal of personal information by data subjects. This may be an extension to the 'Batch Edit' tool, which allows change of ownership of multiple media items.

- A convenient method of exporting media as a 'package' to fulfil data subject requests for data portability.

- The optional presentation of customisable cookie Information and consent messages.

Personally Identifiable Information (PII) Stored

This may include:

- **User Names** – these may include forenames/initials/surnames.
- **User Account Login Names** – most commonly in a '<domain>\<username format>' for AD users. These may be email address or UPN under some configurations.
- **Email Address** – normally used only for informational messages or alerts if enabled in the system configuration, unless used as the 'username' in the user authentication credentials.
- **IP Addresses** – typically the IP address of the device accessing the eStream resources.
- **Passwords** – passwords are stored for eStream 'Built-in' users only i.e. user accounts that only exist locally on the Planet eStream system (e.g. the 'Built-in\Admin' user and other local users created by system administrators) and are encrypted. Passwords submitted in relation to Directory Services authentication and identity e.g. Active Directory users, are NOT stored in the eStream databases.

User Identification is of course an integral part of the system functionality. In most cases users are required to authenticate to access the eStream resources and identity is used to allocate access rights.
User identity is used in relation to media content 'ownership', usage statistics and analytics and participation in quizzes.

IP Addresses are used in relation to filtering viewing statistics i.e. repeated access to the same media from the same IP address does not equate to media views by multiple users. This information may have some value in terms of auditing and security, but would only be available to system or server administrators.

Webservers
The Microsoft Windows Server platform hosting the eStream web site records logs of access to the web site (IIS logs) and these logs include username and timestamp entries, so access can be traced retrospectively if necessary. These logs are available to college server administrators and potentially to eStream support staff by arrangement with IT staff.

Planet eStream Connect Features
Personally Identifiable Information (PII) stored on Planet eStream hosted servers and potentially shared with other users of the eStream Connect features, is confined to the user's 'Name' as submitted by an individual user when they register to use the eStream Connect service.

Data Protection Impact Assessments
None of the limited types of '**personal data**', as stored or processed in connection with the eStream system design and intended operation, are of a '**sensitive personal data**' kind (see 'What information does the GDPR apply to?' above).
As 'High Risk' data is not stored by design or intent, our understanding is that the use of Planet eStream should not intrinsically give rise to a requirement that a DPIA should be conducted.

If the Planet eStream system is configured by the licensed organisation acting as **data controller** to encourage or allow uploading of additional '**sensitive personal data**' e.g. by adding custom metadata fields to the interface for the purpose of storing such information or allowing staff or other users to upload such information in its stated policies, then a formal DPIA should be instigated by the data controller which includes the Planet eStream resource. In this respect, Planet eStream software applications and related systems are acting only as a data processor under the instruction of the data controller.

Third Party Access

Support and Maintenance

Planet eStream authorised support staff can potentially access database contents and archived media by authenticating to an externally available eStream web site. Other members of our staff, such as administrative and accounts staff, do not have this access. All of our support technicians have been CRB checked and work in accordance with signed agreements requiring behaviour in line with, for example, the 'Janet Network Acceptable Use Policy' (https://community.jisc.ac.uk/library/acceptable-use-policy). In most instances media, such as video and images, is not accessed unless the query relates to media access/playback specifically and diagnosis is assisted by this.

Data Sharing

Personal data stored in eStream databases, of the types as indicated above, is not used for other purposes outside of the feature set and intended operation of the eStream system. It is not shared with other third parties and is not processed for other purposes such as marketing or profiling.

Planet eStream web sites in use by individual organisations can be optionally configured by their Administrators to use **Google Analytics** to track site traffic. To protect user privacy, Google policies mandate that no data be passed to Google that Google could use or recognize as personally identifiable information (PII).

Best practices guidance to adhere to this mandate and ensure privacy is maintained is documented online at https://support.google.com/analytics/answer/6366371?hl=en

Google documents its general data protection compliance commitments online at https://support.google.com/analytics/answer/6366371?hl=en

For convenience, Planet eStream provides a mechanism for the data controller to submit code for use with Google Analytics in the eStream site administration interface. The responsibility to use this feature in compliance with Google's terms and conditions and with GDPR and other data protection regulations rests entirely with the data controller of the individual organisation's eStream web site.

Data Retention

Planet eStream Applications

The Planet eStream platform does not remove any archived media content automatically including electronic submissions such as student assessment work. Where the media is uploaded directly to eStream under the student's user account identity, then as long as this 'ownership' is retained and the student has access to the system, the student themselves can manage and also remove these specific media if they desire. The majority of the media assets are uploaded by authorised staff members and the media 'owners' can then manage the items themselves. Powerful tools are however included for Planet eStream system administrators to manage media content and identify and remove unwanted media as required.

Server Log Files

Web server service (IIS) logs and some Planet eStream application software logs may contain PII references. These can provide useful information regarding auditing of access, or attempted unauthorised access, to the system and may provide evidence where security concerns are being investigated. In line with GDPR provisions therefore, these log files should only be retained for a period of time sufficient for useful evidence to be available to a necessary investigation. Disabling of this logging may result in a negative impact to system security and therefore a policy of time limited retention and access restricted to authorised administrative staff only would appear to be a 'best practice'. Automated deletion of log files by scripting is a practical option.

Portability

Planet eStream does allow users with permissions enabled to download media source files via the web interface. The eStream administrators have an option enabled to export media 'Search Results' as an XML format file. A student, for example, can therefore request that an eStream administrator provide them with their own media and associated metadata from the eStream archive in a package that can potentially be moved to another platform if required. The eStream administrator can identify the student's requested file(s) and download each one. Using the search function the items can be retrieved, either using a suitable phrase to return all the requested items in one search result, or by individual searches as necessary. The XML output(s) can then be generated by selecting the orange 'XML' link option, right hand side at the foot of the Search page as in the image below. (see 'The right to data portability' section above).

International Transfers

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to other countries or international organisations.
These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

Planet eStream UVP Hosting Environments

The Planet eStream software suite can be hosted **locally** under the licensed organisation's own infrastructure, or on **cloud based** resources hosted by arrangement with Planet eStream. The nature of personal data stored and its usage is the same under either environment.

Local Hosting

Many Planet eStream installations are locally hosted by the licensed organisation itself. In this case the eStream core services are hosted using Microsoft Server O/S platforms, typically under a secure local 'intranet' environment as deployed by the hosting organisation. The Planet eStream software components are installed by Planet eStream engineers in conjunction with the organisation's IT services. Data processing by Planet eStream is limited to the normal operation of the Planet eStream software features and occasional access for support and maintenance purposes. In most cases the SQL databases are hosted under a MS SQL Express environment on the eStream core server, although the SQL databases may by hosted on a dedicated SQL Server or Cluster at the hosting organisation's discretion. Network security and data access and protection policies are under the control of the local IT service in these cases. Planet eStream does however strongly recommend that secure connections using HTTPS are used for all eStream client connections to the web interface for both local network and external clients.

Additional modules, such as a local Freeview TV recorder or media converter service station, do not store any personal data and are not accessed directly by end user clients.

Cloud Hosting

The hosting of Planet eStream instances in a secure cloud environment has become increasingly popular. The Planet eStream cloud platform is hosted under the Microsoft Azure environment, with the exception of some specific eStream Connect services hosted directly by Planet eStream (see 'eStream Connect features' above). This type of service implementation is commonly referred to as a 'Software as a Service' (SaaS) provision. Microsoft provides extensive documentation regarding Microsoft Azure, its security practices, certifications and GDPR compliance commitments. Detailed documentation is available online from their trust centre resources at https://www.microsoft.com/en-us/trustcenter and for GDPR specifically at https://www.microsoft.com/en-us/trustcenter/privacy/gdpr/solutions

When an organisation chooses to use a Planet eStream cloud SaaS provision to host the Planet eStream UVP software suite, Planet eStream serves as a 'Data Processor' acting on behalf of the licensed organisation which is the 'Data Controller' in respect of the GDPR.

Planet eStream is fully committed to fulfilling its obligations in terms of the GDPR and therefore affirms that it will:

- Only act on the written instructions of the controller, as defined in contractual agreements for use of the service;
- Ensure that people processing the data are subject to a duty of confidence (see 'Third Party Access, Support and Maintenance' above);

- Take appropriate measures to ensure the security of processing (see 'Security' below);

- Only engage sub-processors with the prior consent of the controller and under a written contract Microsoft is the only current sub-processor, as personal data is stored and processed on the Azure platform (see 'Data Sharing' above);

- Assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR (see the 'Individual rights' section above for summarised details);

- Assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments (see the 'Personal data breaches' section above);

- Delete or return all personal data to the controller as requested at the end of the contract; and

- Submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Planet eStream provides hosting for most organisations on its standard cloud platform, which is a multi-tenant architecture resource. Bespoke options based on dedicated VMs are also available as required.

Cloud hosting services for Planet eStream European based customers are located in the Microsoft Azure North Europe data centre (Ireland). Geo-replication of data is paired with the West Europe data centre (Netherlands). Personal data is not transferred outside the EU (see 'International Transfers' above) as part of the Planet eStream SaaS services operation.

Security

The standard Planet eStream cloud platform (and bespoke implementations) benefit fundamentally from the highly secure Microsoft Azure infrastructure on which it is deployed. Detailed information is available from their trust centre https://www.microsoft.com/en-us/trustcenter . Microsoft Azure is certified to ISO 27001, FedRAMP, PCI DSS Level 1, SOC 1 Type 2 and SOC 2 Type 2 security standards.

On the standard eStream cloud platform, each site has its own individual SQL database hosted on Azure SQL server resources, providing a high level of separation for each organisation's data. All connections to Azure SQL Database require encryption (SSL/TLS) at all times while data is "in transit" to and from the database, and databases support Transparent Data Encryption (TDE) for data at rest. All client web connections are secure HTTPS.

Planet eStream subscribes to 'best practices' implied by Article 32, which include technical and organisational and measures to ensure a level of security appropriate to the risk such as:

- Pseudonymisation and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Examples are:

- Appropriate use of encryption (https).
- Maintaining all systems and software with relevant security updates.
- Deletion of personal data as soon as possible, once it is no longer required for the purpose it was collected.
- Penetration testing of Planet eStream software applications and cloud services by accredited third party.
- Deployment of up to date antimalware products.
- Data backups and geo-replication
- Time limitation policies on retention of directly readable log files containing PII e.g. 60 days for IIS logs.

References and Acknowledgements

https://www.itgovernance.eu/eu-general-data-protection-regulation-gdpr

https://www.eugdpr.org/eugdpr.org.html

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

https://ico.org.uk/media/for-organisations/documents/1152/public_authorities_under_the_foia.pdf

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

https://social.luptonfawcett.com/blog/freedom-information

https://www.wrigleys.co.uk/news/education/gdpr-public-authority-status--what-does-this-mean-for-academy-trusts/

https://www.wrighthassall.co.uk/knowledge/legal-articles/2017/11/21/gdpr-individuals-rights/

https://gdpr-info.eu/art-33-gdpr/

https://eugdprcompliant.com/cookies-consent-gdpr/

European Union General Data Protection Regulation (GDPR) FAQ , Microsoft, Oct 2017

An Overview of the General Data Protection Regulation (GDPR), Microsoft, May 2017

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 27 April 2016. Official Journal of the European Union. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

GDPR Articles 4, 5, 6, 9, 13, 14, 15, 22, 28, 32, 33, 34, 35, 36, 55.