Terms of Use & Security

General Data Protection Regulations (GDPR)

This page describes the relationship between HOPS and GDPR. It should not be considered a comprehensive guide to GDPR. (Updated 3 August 2019)

HOPS Data Principles - User's HOPS Accounts

For the purpose of user's HOPS accounts:

- the "User" or "Individual" is the employee or volunteer or other person related to the HOPS's clients to whom the data relates.

- the "Data Controller" is HOPS.

- the "Data Processor" is HOPS.

Data stored and processed by HOPS relating to users' accounts includes the user's names, username, password and login records. For some users their title and gender is also stored.

This data is used stored under the legal basis for processing of 'legitimate interest' in order for HOPS to deliver services to its clients, for which HOPS users are or have been employees, volunteers, contractors or involved in some other way. This data will be stored for as long as it is necessary to deliver the legitimate needs of the client. In some cases, for insurance requirements, this can be as long as 40 years.

HOPS also keeps records of users' activity when using its services. This is for the purpose of monitoring and safeguarding security of HOPS's services, and also to assist clients in audit/investigation work. Login records are kept for approximately 5 years. Other such data is kept for approximately 1 year and then deleted.

HOPS is obliged to meet its obligations under GDPR. HOPS employs staff and contractors to assist in the management of the business and the website. Such employees and contractors are bound by the same obligations as HOPS.

HOPS Data Principles - Records Created by Clients

For the purpose of data about users stored in HOPS by client organisations:

- The "User" or "Individual" is the employee or volunteer or other person related to the Data Controller to whom the data relates. Users generally carry out work for the client organisation, either in an employed or volunteer capacity, or are related to the organisation in some other way.

- The "Data Controller" is the client organisation, often a heritage railway or museum. Clients use HOPS to assist in the delivery of their legal and moral obligations relating to the operation of the their business in compliance with laws such as the Health & Safety at Work Act, the ROGS Regulations, PUWER, COSHH, GDPR, etc. The Data Controller is obliged to meet their obligations under the GDPR, and to assist HOPS in meeting its by proper use of its systems and services. The Data Controller is responsible for ensuring there exists a legal basis for processing the user's data other than 'consent'.

- The "Data Processor" is HOPS. The Data Processor is obliged to meet its obligations under GDPR, and to assist the Data Controller in meeting theirs wherever possible. Apart from trivial matters, HOPS will only take actions on the data belonging to the Data Controller on the HOPS Admin's (or their representative's) instructions. The HOPS Admin is considered the client's Data Controller's representative to HOPS. HOPS employs staff and contractors to assist in the management of the business and the website. Such employees and contractors are bound by the same obligations as HOPS.

HOPS also takes appropriate measures to ensure the security of data. More details

All data is owned by the Data Controller, and HOPS only processes it in line with the actions and expectations of the owning Data Controller.

The subject matters of the processing are the users (staff and volunteers) and the operational and commercial activities of the clients.

The duration of the processing is ongoing, with no defined end date.

The nature of the processing is administrative tasks relating to the management of the business and the co-ordination of staff.

Personal data processed includes contact information, emergency contacts, medical, working arrangements, competences, HR records, incidents, rosters, commercial activities, cash, asset management, timetables, and other facets of business and railway operations management.

Records are kept for a period after the user ceases work with the organisation. This will be for a period as long as it is necessary to deliver the legitimate needs of the client. In some cases, for insurance requirements, this can be as long as 40 years.

GDPR Principles

Under the GDPR, the data protection principles set out the main responsibilities for Controllers and Processors.

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

HOPS processes data in accordance with well-established processes for the administration of heritage railways and other museums and tourist attractions. The outcome of these processes is transparent to individuals via the website interface in the form of the information output, ie, rosters, reports, etc.

Not all output of processing data is visible to all users, access is controlled by the Data Controller (the client organisation). For example, if a user is over 60, the fact that this is recorded in HOPS will be clearly visible to the user. However, a report showing all users over 60 will have been constructed using an individual user's data who is over 60, but it would be contrary to other more significant data protection principles to display this report to all those mentioned in it.

Some data about subject users is stored in HOPS by clients and is not generally visible to the subject user, but will be disclosed by the Controller on request where Article 13 of GDPR requires.

There are six legal baseis for processing. Some illustrative examples are given below of how the legal baseis might apply to various types of data held in HOPS.

The Data Controller is responsible for ensuring that data held has a legal basis. Decisions on which legal basis applies are taken by each client, and each could legitimately come to different (valid) conclusions. This page merely provides illustrative examples rather than being specific or prescriptive about each type of data, apart from in stating that legal basis of 'consent' must not be used to store data in HOPS.

(1) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

Consent is generally not a suitable legal basis for storing information relating to the management of staff working in an organisation. It is not permitted to use this as a legal basis for storing data in HOPS.

Working for an organisation, including as a volunteer, brings a lot of obligations to the organisation that are equivalent to if the person was an employee. It is widely-required to store and process data in connection with a person's employment, the legal basis for doing this would be 'legitimate interest'.

It is wise, not only for the purpose of GDPR but also for general management and safety, for organisations to routinely remind users of the data they hold about them, particularly contact information, and for the user to confirm it remains accurate. When doing this, it is recommended that organisations DON'T ask for consent to store this data. In asking for consent a user might surmise that that is the legal basis on which it is being held, which is not the case. Legitimate Interest should be the legal basis on which information about employees (including volunteers) is held, and must be the legal basis on which such data is stored in HOPS.

One key reason for Legitimate Interest being a better legal basis than Consent is a user can withdraw their consent. It would be extremely difficult to justify removing a user's records from systems used in record-keeping in a safety-critical business (ie training/competence records, etc). An employee must provide their data either to satisfy legal requirements (right to work, tax, NI, ROGS, etc) or to satisfy the legitimate interests of the organisation to manage safety.

(2) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Similarly to (1), with regards to contracts of employment, storing and processing data regarding that employee is necessary and appropriate.

(3) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

Most HOPS clients are railways that work within the ROGS legislation. Whilst storing and processing of data of this type is not an explicit interest of ROGS, the requirement to manage a safe and well-governed railway is, and availability of data such as that stored and processed in HOPS is widely considered to be appropriate in the discharging of a duty holder's responsibility under ROGS. HOPS does not deliver any safety critical data such as that required in the operation of signalling systems, etc.

(4) Vital interests: the processing is necessary to protect someone's life.

HOPS does store medical and allergy information, and also emergency contact information, which is used in emergencies such as medical emergencies, and which employers would probably struggle to defend not storing for the purpose. However, HOPS does not presume that HOPS is a sufficiently major tool in this respect to justify claiming this legal basis applies.

(5) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

This legal basis does not apply to HOPS, apart from in assisting railway clients in meeting their obligations under ROGS.

(6) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

This is the most appropriate legal basis for the storage of data related to users of HOPS.

The processing that takes place on data stored in HOPS is necessary to achieve the information outputs and services that HOPS's clients require. The importance of this information to the client varies, ranging from 'interesting' to 'business critical'. GDPR does not require processing of data to be 'essential' and therefore processing data to produce 'nice to have' information is permitted.

HOPS and its clients balance what storage is reasonable and practicable with what is a reasonably required outcome. There are

other methods of processing similar data, such as Excel spreadsheets, etc, but as a tool designed for the purpose of managing such data, HOPS is considered the most appropriate tool for the task.

Special Category Data - HOPS stores and processes a small amount of 'Special Category Data' under the 'health' category, as it stores medical and allergy data. If a data controller stores other 'Special Category Data' in HOPS (ie using 'remarks' fields etc) then the Data Controller must make sure there is a legal basis for doing so.

Criminal Offence Data - HOPS does not explicitly provide for the storage of Criminal Offence Data, although several clients use the 'competence' facilities to store CRB/DBS status. If a data controller stores other 'Criminal Offence Data' in HOPS (ie using 'remarks' fields etc) then the Data Controller must make sure there is a legal basis for doing so.

b) 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;

Data is collected by the Data Controller and stored in HOPS on their behalf. The Data Controller is responsible for collecting data that is defensible in terms of its congruence with their organisation's operations and requirements.

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

The Data Controller is responsible for determining what is volume and range of data is adequate and relevant to store based on the detail of their operation and the purpose for which the data will be used by them.

HOPS provides fields for storage of data based on best practices and information suggested by its user community that is appropriate to store, but in doing so does not guarantee that storing such data is relevant to every client's operation or defensible under GDPR.

HOPS does not process data for any purpose other than that of the client organisation, so clients may be assured that if they determine that the purpose and processing of storing their data in HOPS is compatible with their organisations requirements, no additional, potentially incompatible processing will take place.

d) 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;

The accuracy of data in HOPS is the responsibility of the Data Controller. HOPS will intervene and assist users in having inaccurate data or inappropriate data corrected when all attempts to resolve this between the client and user have been exhausted (in HOPS's view).

e) 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

Data subjects are identifiable from data held in HOPS. Informal consultation with clients as to the length of time that various types of information should be stored indicated a minimum of 10 year period after the usable date of the information has passed (ie, save rosters for 10 years). This was heavily influenced by the requirements of compliance with ROGS.

HOPS started storing data for railways in January 2010, so even the oldest data is under 10 years old. As HOPS is approaching 10 years old, HOPS is currently consulting with its clients regarding an appropriate deletion policy. Early indications from this consultation are for a retention period of less than 10 years for some existing data. HOPS will continue to work with all its clients to ensure continuing maturity of data retention policy.

f) 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.

Server security is important in ensuring compliance with this principle, details of which are available here.

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

Compliance with the principles is the responsibility of the Data Controller. HOPS makes the commitment above to assist with this.

Individuals' Rights

The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. It is the responsibility of the Data Controller to inform users. In the context of HOPS this is more significant in the case of "offline" users.

The right of access

Individuals have a right to access their data. This can be facilitated through the normal HOPS web interface. Data Controllers must be prepared to make data accessible to offline users, the simplest way may be to make offline users into live users for the purpose.

The right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.

An individual can make a request for rectification verbally or in writing and the Data Controller has one calendar month to respond to a request. (In certain circumstances a data controller can refuse a request for rectification, but should communicate the rationale for

this with the user.)

HOPS will intervene to assist a user to correct or erase inaccurate data if all avenues of enquiry with the Data Controller have been exhausted. HOPS will act impartially in the best interest of the user and the Data Controller.

The right to erasure

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing. Data Controllers have one month to respond to a request.

The right is not absolute and only applies in certain circumstances. One of the examples of a circumstance in which it doesn't apply is if the data is being stored and processed to comply with a legal obligation (ie ROGS), another is for the establishment, exercise or defence of legal claims (ie retrospective insurance or employment claims). (This list is not exhaustive.) It is probable that HOPS and its clients will be storing and processing data for these purposes, so it is likely that many parts of HOPS data would be excluded from the right to be forgotten.

Due to the safety nature of many of HOPS's clients, HOPS will not delete its clients' data under this rule unless compelled by law-enforcement to do so.

The Right to Restrict Processing

Individuals have the right to request that the processing of their personal data is restricted in the following circumstances:
- the individual contests the accuracy of their personal data and you are verifying the accuracy of the data;
- the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- you no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to you processing their data under Article 21(1), and you are considering whether your legitimate grounds override those of the individual.

In any case where an individual requests the processing of their data is restricted, the Data Controller must either remove it from HOPS or liaise directly with HOPS regarding the restriction. Data which is restricted from processing IS still permitted to be stored, and 'archived' users would fall into this scenario.

The Right to Data Portability

HOPS will do its best to assist Data Controllers with requests for structured-format reports of user data for portability. It is generally expected that Data Controllers will deal with these requests, wherever possible, using the Reports function in HOPS.

The Right to Object

Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

HOPS does not process for these reasons, and generally its clients do not either. It is expected that a user exercising their right to object would be dealt with by the action of the Data Controller.

Users have various rights related to automated decision making including profiling

HOPS does carry out some automated decision-making, such as in the allocation of turns in rosters. Due to the nature of user availability and the nature of rosters, sometimes this appears random, and sometimes patterns appear which become apparent to those affected, ie "I'm always rostered on Wednesdays". Although this is a mathematically sound outcome for the economy of covering the most turns, Data Controllers (and their roster clerks) should be receptive to users raising this as a concern and amend the rosters accordingly.

If you would like more information about HOPS please contact us.