GDPR Compliance

HTK document

Statement of HTK's GDPR compliance policies and processes

Version 1 | 18 April 2018

Author: John Martyn

Contents

The EU General Data Protection Regulation (GDPR) came into force on 25th May 2018. GDPR changes the way in which organisations need to handle data.

At HTK we have undertaken steps to ensure that we are GDPR compliant and have developed our Horizon platform to make it easier for our clients to comply with their obligations under GDPR.

The following guidance relates to data processing that is subject to the GDPR. GDPR will generally apply only to clients in the EU or those outside the EU who process data relating to individuals from the EU regardless of where the client is based. If you are in any doubt as to the applicability of GDPR to your processing you should speak to your legal advisers.

Data Processor

HTK is a Data Processor within the meaning of GDPR and our clients remain the Data Controller in respect of the personal data that they input into the system. Our clients remain in control of the way in which we process data on their behalf at all times.

Our terms and conditions of business form the basis of the data processing contract between HTK and our clients. This document sets out more detailed information about the services we provide, how we comply with the requirements of GDPR and how our clients can utilise the Horizon platform as part of their compliance strategy.

Use of Personal Data

Our client remains at all times in control of the personal data input into Horizon. HTK never use this data for their own purposes and will only ever access and use our client's data to the extent necessary to provide the services agreed with clients. For example, our support team may be asked to look at specific issues that are raised with them.

Security of Data

HTK has in place detailed physical, technical and procedural measures to protect our client's data. These measures are constantly reviewed and adapted to provide appropriate protection for our client's data.

Below is a brief summary of the measures that we currently have in place. If you require more detailed information, please contact us directly.

Physical Security

HTK stores client data in multiple, secure, data centres within the EU. HTK does also use data centres in the US but these are used solely in respect of US customers for US based data. The data centres all have multiple physical controls that restrict physical access to sensitive and restricted areas of the data centres. HTK does also use data centres in the US but these are used solely in respect of US customers.

Technical Security

Access to the Horizon platform is via a secure connection. There are multiple layers of intrusion protection, intrusion detection and firewalls between the internet, our application servers and the databases. Access is limited to users who have been authorised by our client with two factor authentication available to strengthen access controls if required.

Procedural Security

HTK is ISO27001 certified and follows the strict information handling requirements of these standards.

HTK internal policies and controls restrict access to the application and database servers to those who require access.

All access is monitored. All staff with access to databases undergo specific information security and data handling training prior to being given access to client data.

Data Subjects' Rights

The GDPR strengthens the rights that individuals have in respect of the way that data controllers process their data. The Horizon platform makes it easy for our clients to comply with these new rights and we summarise below how the key rights can be addressed with the Horizon service.

Subject Access Requests

Data subjects have similar rights under GDPR to the current law to access copies of information that

data controllers hold about them through a subject access request (SAR).

HTK makes it easy for its client to handle SARs through the Horizon platform. If you have direct access to Horizon then you can search the relevant information that the requestor is looking for and export this in a suitable format to provide to the data subject. If you do not have direct access to Horizon then you can put in a support request to HTK for a copy of such data and we will provide a copy of the requested data held within Horizon within 10 days of a request being received from a client. The client though remains responsible for ensuring that HTK is notified of the request within sufficient time for the overall one calendar timescale to be met by the client as required under GDPR.

As the data controller our client remains responsible for handling SARs and HTK will not take any action in respect of an SAR unless in accordance with specific instructions from our client. If HTK receive an SAR direct from a client's data subject they will be referred back to the client.

The Right of Erasure

The GDPR gives data subjects' new rights to have data about them erased in certain limited circumstances. Whether and the extent to which such a request is actioned is a matter for our client to determine. Once permanently deleted, such data cannot be restored.

If you have direct access to Horizon then you can delete the contact record via the UI, and you will also then need to delete the contact from the re-cycle bin at the same time in order to completely remove the data record. If you do not have access to Horizon, you can put in a support request to HTK for deletion of a contact (note that the request MUST come from a person with the appropriate authority to request the deletion). We will then delete the contact on your behalf and confirm deletion within 5 days of the request.

HTK will not delete data other than in accordance with the specific instructions of our client.

HTK run a 7 day back up cycle and then backed-up data is stored for 2 years. When restoring data from backups, any data which has been deleted in live environments, is also deleted from the backup data as part of the "restore" process.

The Right to Rectification

GDPR allows data subjects to have their data corrected when it is wrong. If you have direct access to Horizon you can manage these requests directly within Horizon. If you do not have direct access then you can put in a support request to make the appropriate modification and this will be

actioned within 10 days and confirmed to you. HTK will not modify client data other than in accordance with the specific instructions of our client.

Third Party Transfers

HTK does not use any third parties to process any of the personal data stored within the Horizon system, except as noted below, and, unless otherwise required by law, will not transfer any of this personal data to any third party other than in accordance with the specific instructions of our client.

HTK uses a 3rd-party organisation, oneall.com, to interface with social networking sites. This involves the passing of an identifier for the user, but no additional data will be transferred without the user's explicit consent.

International Transfers

HTK does not transfer any personal data stored within the Horizon system outside of the European Economic Area unless specifically requested by our client. However, our clients who have direct access to the Horizon platform can access this from anywhere in the World and our clients are responsible for any transfers that may arise from such access.

Retention of Data

In accordance with our terms of business, if requested by you within 30 days after the effective date of termination of a purchased service, we will make available to you for download a file or files of your data in .csv format along with attachments in their native format. After such 30 day period, we shall have no obligation to maintain or provide any of your data and will thereafter, unless legally prohibited, delete all of your data in our systems or otherwise in our possession or under our control. We will however retain copies of your data on our backups for up to a 2 year period, but when restoring data from backups, any data which has been deleted in live environments, is also deleted from the backup data as part of the "restore" process.