timesheet portal

anfold software

Data Protection Guide

Anfold Software Ltd is the provider of Timesheet Portal, which is a software as a service (SaaS) offering. Due to the nature of the some of the functionality of this software (e.g. payroll processing, HR record keeping), we have the ability for our customers to store personal data relating to other customers. We are a Data Processor and we are registered with the ICO. Our customers usually fulfil the role of Data Controller, but in some cases may act as a Data Processor themselves.

Our standard terms and conditions outline the duties and obligations of our customers and ourselves. These can be found online in the support section. This document provides further details on data security and internal processes where personal data is involved.

For further information please contact our Data Protection Officer:

Name: Michael Gois

Email: mgois@anfold.com

Data Collection

We do not collect any personal data from your users for our own use. We are the Data Processor and you are the Data Controller. It is entirely up to you what data you wish to put in our system, and what fields you wish to make mandatory, and what permissions you assign to your account users which may give them access to the personal data of Data Subjects.

Storage & Archiving

Where is the primary data stored?

Primary data refers to the data contained within the Timesheet Portal application. This includes all data which is entered through the user interface, import files, API and any other areas in which the data becomes available through the interface. This data may be entered by administrators or data subjects themselves, or through any automated system processes that you may have in place to import data into our system.

For reasons of redundancy and scalability, we host your data in multiple places concurrently. These include our dedicated hosted servers housed in a secure data centre with ISP UKFast as well as other services provided by Microsoft Azure and Amazon Web Services.

How we handle data provided to us directly from customers

During implementation and other ad-hoc support or development projects in which we engage with our customers, we may receive files from you containing personal data. These may be stored on our local machines or our servers in the office. Our

policy is to not store any personal data on any of our disks which are not encrypted, and staff are aware which disks are safe to store personal data on.

After an implementation, our policy is to delete the implementation data after a period of 3 months. (Please see data rention policy for information on how we handle primary data)

Archiving

Apart from our regular backups, we do not archive your data for any other purpose. We keep backups for a period of 3 months.

Security

Access to personal data

Within our organisation, our support and implementation team may access your account. This is a requirement in order for them to fulfil their role so that they can provide support to our customers. This access is logged.

During trial and for your first 3 months after commencing a subscription with us, your sales executive may have access to your account. This is essential as typically they provide a crucial role in helping refine your requirements and relaying these requirements to the implementation team.

Access to servers containing personal data

We maintain restricted access to servers and databases. Access is limited to key senior members of the technical team, and access to servers is audited. We also maintain a log of all people who have access to servers. If a member of staff leaves or their role changes such that they no longer require access to servers, their credentials are promptly revoked.

Virus Scanning

We use virus scanners on our production servers and in our internal network. Virus definitions are updated on a weekly basis.

Working with sub-contractors

We do not typically engage with sub-contractors who could have access to personal data. However we would ensure a suitable contract exists and training is provided which addresses the need to protect any personal data dealt with by the sub-contractor.

Security Procedures

Your data is stored within the software that we provide. Hence our focus on security procedures is mostly based around ensuring good practices during development of the application and in keeping the production environment secure.

Our development team are trained to understand how attacks can occur and how to write code that is not susceptible to such attacks. We also conduct regular code reviews by a senior member of the team to ensure that good practises are maintained.

As part of PCI compliance, we undergo quarterly vulnerability scanning. These are automated scans that test our server for known vulnerabilities. In addition to this, we also undergo annual web application penetration testing. This testing comprises of manual and automated tests whilst logged in to the system, with a specific focus on ensuring personal data cannot be compromised by an unauthorised user.

Data in transit

All data, including personal data is always secured when in transit over public networks. Emails and data storage are processed through Microsoft's Office 365 suite, and transferred over SSL/TLS. Data is encrypted

We use SFTP for FTP transfers.

All our internal disks on desktop workstations and laptops use Microsoft Bitlocker to encrypt files using 128bit AES.

Intrusion Detection

We operate hardware and software based firewalls across our internal and production networks. Currently we are working on new processes for monitoring and identifying intrusions on the servers and databases, and will provide further information once our new processes are established.

Report of a data breach

In the event of a data breach, we have procedures in place on our system which will allow us to email all registered DPOs for our customers, the Data Controllers. As per our obligations under the GDPR, we will report a breach to all affected Data Controllers without delay, and notify the ICO within 72 hours. If you have not registered a DPO contact on our system, then we will email the primary administrator on the account instead.

Central Record of Processing Activities

Anfold Software maintains a central record of processing activities. We do not maintain a list of the individual personal data field that each Data Controller uses, as Data Controllers have complete control over what personal data they enter relating to their Data Subjects and also what fields they ask their Data Subjects to complete on our system.

Destruction of Data & Contract Termination

Your responsibilities for deleting data

By default, our system does not fully delete a user's record when you delete them. Instead, we mark their record as deleted so that you are able to run historical reports. For example, one of your employees may have left your company 6 months ago, but you may still wish to run a report to identify the gender of all your active employees in the last 12 months.

If one of your data subjects makes a request to exercise their right to be forgotten or wish to know what personal details are held about them, we will relay this request directly to you. As you are the data controller, this is your responsibility. We do however provide features to facilities your responsibilities as a data controller. For example, you can use our system your data subjects to request their right to be forgotten, giving you the ability to track these requests, receiving notifications of them and mark them as complete. Additional features are being developed and we will update our help guide with all relevant GDPR features in the coming weeks.

How is data destroyed

We do not typically work with printed data, however if there was a requirement to print data which contained personal data, our policy is to shred such documents.

With regards to digital data, a deletion process will result in overwriting any records containing personal data with blanks. When a customer account is terminated, we will fully remove all data records from the database.

Termination of contract

When you terminate your contract, unless otherwise specified, we will irretrievably delete all your data after a period of 3 months. This includes personal and other data, but excludes billing data. This is clearly outlined in your terms.

Sub-Processors

We do not host our own servers or redundant storage facilities in-house, therefore we engage with several sub-processors in which we store personal data on. All our sub-processors are GDPR compliant.

Security measures of sub-processors

As part of our compliance policies, we have undertaken an assessment on each of our sub-processors to ensure that they follow similar security measures which are deemed acceptable for safe-guarding personal data.

Appointment of new sub-processors

If we engage with a new sub-processor, we will notify your DPO, providing you with 30 days to object. If you object to our appointment of sub-processor, you may end terminate your contract early. This is explained within our terms.

Transfers of personal data

Application data transfer

Due to the technical architecture of our system which is a requirement for redundancy and scalability, when personal data is accessed, created or modified, it will be transferred between different components of our system, and in some cases this will be over the internet between different physical sites. All digital transfers are kept within the EU.

Internally, we may transfer personal data between departments. For instance, during implementation, a customer may send data for importing into the system to their sales executive, who may in turn send this information to the implementation team. Such data transfers will be performed over secure email connections, or by saving the data to local and cloud-based storage providers. Our internal policies prohibit us from storing any customer data on non-encrypted disks.

Training

General Data Protection

Our staff have all had online training sessions on the principles of GDPR compliance and how to deal with personal data. Our staff are also aware that unlawful access to personal data is prohibited.