# Planday and GDPR compliance

## GDPR

In lieu of the General Data Protection Regulation (GDPR), we've had questions from customers about what GDPR is and what Planday is doing to comply. To answer some of those questions and make the implications of GDPR clear, we've outlined what exactly GDPR is below. The information here is meant to used for informational purposes only, and not meant to serve as legal advice. You should work closely with legal counsel to determine exactly how GDPR might affect you.

### Planday's commitment to security and data protection for GDPR

## Planday's commitment to security and data protection for GDPR

From our executive team to our developers, everyone at Planday takes the security of our product and the protection of our customers' and employees' personal data very seriously. Our customers trust us with their data, and protecting that is crucial to running our business.

We're actively working with our customers to fully understand their data processing and privacy needs. Additionally, we're working with a specialist organisation to ensure that we're ready for the changes brought in by GDPR.

We approach data protection from two different angles: internal processes and technical development. In short, we do everything we can to ensure we have the right people, processes

and training in place to protect our customers' data, while also ensuring our product is technically airtight.

## Technical commitment

From a technical perspective, we go to great lengths to ensure that we protect our system from internal and external abuse with the controls laid out in this article. These controls play a big part in our GDPR compliance, while also helping our customers become GDPR compliant by ensuring the storage of employee data in Planday is up to GDPR standards. From a purely infrastructure perspective, we ensure the following: that the Planday system is protected from external attacks, that the data in the system is protected through encryption, and that we use data management processes to protect data from internal and external abuse. We have a third party carry out extensive penetration tests and a security audit on a regular basis.

Planday is a certified CyberEssentials holder, which is a UK government-backed cyber protection scheme. We're also registered with the Information Commissioner's Office (ICO) and Datatilsynet (the Danish data protection supervisory body). Additionally, Planday is ISO27001 certified.

Of course we also comply with local data security and trading regulations in all our markets.

## Process commitment

GDPR is a part of our enterprise risk management, meaning we think about GDPR compliance as part of the methods and processes we use to manage risks and achieve our objectives as a company.

As a part of this compliance, Planday only processes data as per our Data Processing Agreement. All the data we process is protected in our infrastructure and SaaS systems– meaning the data we process never leaves a secure system.

Additionally, all access to customer data is protected by roles and permissions within the Planday system. Planday employees can only access data on a need-to-know basis, and according to "the principle of least privilege," which means Planday employees have the minimal level of access to data in order to do their job.

When we process and access data, it's always with consent– whether it's in accordance with our Data Processing Agreement or with explicit customer consent. That ensures we fulfill our

legal obligation to our customers to protect their data at all times.

All access to customer data within the Planday product is also via consent only. For example, when a Customer Success team member needs to access a customer's Planday account, the customer must give permission for the CS team member to access that data.

We require all our employees to complete data protection training, with an emphasis on how data protection relates to GDPR. Employees are routinely trained on new processes and procedures, and retrained on any subsequent changes.

Additionally, we require that each department document any process that relates to the processing of personal data. To protect our system against internal abuse, we also ensure Planday employees are given the minimum access to data required to carry out their role.

We believe GDPR is incredibly important, and will continue to review our data protection processes on an ongoing basis. We don't see GDPR as a one-off project, but as an ongoing commitment to data protection and privacy.

### What is GDPR?

## What is GDPR?

As the General Data Protection Regulation (GDPR) gets closer, we've received questions from customers about what GDPR is and what it means for them. To answer some of those questions and make the implications of GDPR clear, we've outlined what exactly GDPR is below.

The European Parliament and Council passed GDPR in April 2016 in order to protect European Union citizens' personal data. The regulation will take effect on May 25, 2018 and will replace legacy regulations, as well as introduce several new laws and non-compliance penalties.

### Scope

One of the biggest differences between GDPR and older data protection laws is the scope. Any company located in the EU collecting or processing data must comply, as must companies collecting or processing data belonging to EU citizens (regardless of where the company is located).

UK citizens will still have the same data protection rights post-Brexit, meaning, UK businesses should prepare to fully comply with GDPR by May 25th.

## Goals

- **Individual control over personal data**. The main goal of GDPR is to give individual citizens more control over their personal data and how that data is used.
- **One, simplified regulation**. GDPR replaces several older data protection laws (i.e. The Data Protection Directive), and unifies EU laws under one regulation. The language in the GDPR regulation is quite easy to understand, making it easier for companies to comply.
- **Higher compliance rates**. GDPR was created with the intention of higher levels of compliance and so has much harsher penalties than previous data protection laws.

## Major changes

Many of the major changes that come with GDPR fall under several overarching themes:

- **Anonymization/pseudonymisation**: All personal data should be anonymized when possible. That means information from which it is possible to identify an individual should be either removed from a data set or encrypted, so individuals remain anonymous.
- **Right to be forgotten**: Companies have to erase personal data if a customer requests it, and if certain conditions are met (including a company's noncompliance).
- **Right of access**: Individuals have the right to know how their data is being used. Data controllers and processors must explain how personal data is used, who it's shared with and why– upon request.
- **Data portability**: Individuals have the right to easily transfer their data from one provider or processor to another. Companies must give individuals their data in an easy to read format or pass it on to the provider, when requested.
- **Data breach notifications**: GDPR has very specific requirements for what an organisation must do in the event of a data breach. Notifications must be sent to anyone affected within 72 hours.
- **Appointment of a Data Protection Officer (DPO)**: Public authorities, systems that have large-scale user monitoring (like behaviour tracking tools), or companies that process large amounts of data must have a DPO. A DPO's purpose is to lead their company towards compliance and act as the primary liaison with local and EU data authorities.
- **Privacy by design**: GDPR strives to protect personal data as a fundamental right. Because of that, designing products and services with data protection in mind will now be a legal requirement.
- **Legal basis for data use**: Organisations must be able to demonstrate that they have relied upon one of the six legal grounds for using personal data.

### What are the penalties for non-compliance?

Organisations who are found to be non-compliant may be fined up to €20 million or 4% of their total global turnover of the preceding financial year, whichever is higher. Member states may also impose their own rules and fines in addition to the specific penalties detailed in the GDPR. Read more about the consequences of non-compliance here.

### Who does GDPR apply to and what implications does it have?

## Who does GDPR apply to and what implications does it have?

The General Data Protection Regulation (GDPR) grants new rights to EU citizens about the use of their personal data, which means businesses now have to handle their customer and employee data differently.

### Who's affected by GDPR?

Any organisation that handles data belonging to EU citizens is affected by GDPR. There are a few situations in which processing personal data isn't regulated by GDPR, such as:

- Activities in Title V of the Treaty on European Union (TEU). These laws are designed to foster policy cooperation between EU members.
- Actions by authorities. Legal authorities working on crime prevention, investigation or prosecution are exempt.
- Activities that aren't regulated by EU law. This includes things like state security and other activities that are outside the scope of EU law.

Organisations outside the EU that process EU citizen data also have to comply with GDPR, making the impact of GDPR truly global.

The regulation also states that organisations that send their data outside of the EU to be processed are still subject to the GDPR. The bottom line is that most organisations that process personal data will have to comply by 25 May 2018.

UK citizens will still have the same data protection rights as EU citizens post-Brexit. That means UK businesses should prepare to fully comply with GDPR by May 25th.

### Appointment of a Data Protection Officer (DPO)

GDPR will require ongoing work from all affected companies. As part of that, some organisations will need to have a Data Protection Officer (DPO), who will handle all GDPR issues and ensure compliance. Public authorities, systems that have large-scale monitoring (like behaviour tracking tools) or companies that process large amounts of data must have a DPO.

## Rights granted to EU citizens under GDPR

GDPR gives EU citizens more control over how their data is used by third parties. Some of the new data rights have long been best-practice in the EU for over a decade, but are formalised by GDPR. Others are new concepts, and require organisational and procedural changes.

## The Right of Access

The Right of Access gives individuals the option to see how their data is used and processed. Anyone can request details about why their data is being used, where and by whom. EU citizens are also granted the right to make formal complaints, and it's mandatory that organisations notify their customers that they have the right to do so. As part of this, automated decision making (like profiling) must be made transparent.

## The Right to be Forgotten

The Right to Erasure, also called the Right to be Forgotten, is an update to previous laws– namely the 1995 Data Protection Regulation, which gave people the right to ask a data processor to delete their data in a more limited way.

GDPR strengthens that ability, giving EU citizens the right to have personal data they hold erased from any third party data processor that's used by the data controller. That means their data cannot be shared further, and any links or copies must be deleted. In order for someone's data to fall under the The Right to be Forgotten, the data must be considered non-necessary, their consent to their data being used must be withdrawn or the data must have been illegally processed.

## The Right to Portability

If someone requests to see their data, an organisation must provide a copy of the data in an easy to understand format. EU citizens can also request that any business send their data to another organisation, so no one is locked into one data processor.

## Protecting customer data

Article V of the GDPR covers how data can be processed in order to protect customers. This section also outlines rules for data collection and storage and boils down to the requirement that personal data should be processed lawfully, fairly and in a transparent manner. One of the primary rules says that data can only be used for the specific purpose it was collected for.

Data can also only be collected and processed if one of the following conditions has been met:

1. The individual has given consent for his or her personal data to be processed for specific purposes
2. Processing is necessary for to fulfill a contract between the processor and the individual
3. Processing is necessary for the data controller to follow the law
4. Processing is necessary in order to protect the vital interests of the individual or someone else
5. Processing is necessary for public interest or carrying out official duties
6. Processing is necessary for the legitimate interests of the data controller or a third party

Because GDPR is designed to protect EU citizen data, it gives them the right to withdraw consent for data processing at any time. Article VII states that withdrawing consent for data processing must be as easy as giving consent.

## Anonymisation

GDPR outlines how data should be anonymised in order to protect individuals when there's no need to process their personal details. Basically, that means personal identifying information is removed from a data set so individuals remain anonymous (e.g. removing names, addresses, and personal identification numbers from data).

## Pseudonymisation

GDPR also recommends the pseudonymisation of data. This means the data can't be traced back to an individual. If a business complies with the pseudonymisation aspect of GDPR, they can actually be granted special privileges, like using that data for broader purposes than those for which it was originally collected.

## Steps to prepare your business for GDPR

# Steps to prepare your business for GDPR

The General Data Protection Regulation (GDPR) affects any business that handles data belonging to EU citizens. The new regulation replaces the 1995 Data Protection Directive and introduces new rights that are designed to protect personal data. On May 25, 2018, organisations that are not prepared could face hefty non-compliance fees.

Don't start panicking yet, though. We have some handy tips below on how you can get your business ready for GDPR. This advice is meant to act as a suggestion. For legal questions on how you should comply, please consult an attorney.

## Understand the purpose of GDPR

The main goal of GDPR is to give individual citizens more control over their personal data and how that data is used— which is great news for consumers. Several sections of GDPR cover how a business must handle data and what kind of data is protected.

Make sure to inform your employees about the implications of GDPR. In certain situations, large organisations may find themselves in need of a Data Protection Officer (DPO), whose job it is to do the following:

- Educating employees on why GDPR compliance is important
- Training staff involved in data processing
- Auditing our systems to ensure compliance and addressing problem areas proactively
- Serving as the point of contact for GDPR authorities
- Maintaining data processing records, which must be turned over to customers if asked

## Steps to make sure you're ready for GDPR

## Evaluate if you have to comply with GDPR

Chances are, you'll have to comply with the new regulation. One of the biggest differences between GDPR and previous data protection laws is the territorial reach of the new regulation. GDPR applies to all companies that handle personal data belonging to EU citizens, regardless of where the company is located.

## Understand the new rights every EU citizen has

GDPR grants EU citizens new rights when it comes to their data. The most significant of these rights include:

- Right to be Forgotten: Companies have to erase personal data if a customer requests it, and if certain conditions are met (including a company's noncompliance).
- Right of Access: This article gives individuals the right to know how their data is being used. Data controllers and processors must explain how personal data is used, who it's shared with and why– upon request.
- The Right to Portability: This gives individuals the right to easily transfer their data from one provider or processor to another. Companies must give individuals their data in an easy to read format or pass it on to the provider requested.

## Take inventory of your data

In order to understand the changes GDPR might mean for your business, you need to first understand how you use and process data internally. Below are a few questions that can serve as a starting point for your data inventory:

- What type of customer information do you process?
- How much of it is highly sensitive or identifying data?
- What information is absolutely necessary to running your service?
- Which third parties do you share customer data with?
- How do you get consent from customers to use their data?

## Review your consent process

Under GDPR, you can only collect and process data if it's "necessary" for you to do so. GDPR outlines six reasons why you might need to process data:

- The individual has given consent for his or her personal data to be processed for specific purposes
- To fullfill a contract between the processor and the individual
- The data controller must processes the data in order to follow the law
- To protect the vital interests of the individual or someone else
- To protect public interest or carry out official duties
- It's in the legitimate interests of the data controller or a third party

## Get your privacy statement ready

Another important step is to prepare a ready-to-go privacy statement. Because of the Right of Access and Transparent Information, a business must share specifics about data use with customers. A privacy statement should include GDPR-required information with customers.

## Think about data protection by design

GDPR strives to protect personal data as a fundamental right. Because of that, designing products and services with data protection in mind will now be a legal requirement. GDPR requires data processors to use state of the art technology to ensure everyone who uses their services can meet the highest requirements of data protection. Start changing the way your business approaches problem solving, design and development so privacy and data protection are baked into the foundation of your processes.

## Make sure you can access individual data upon customer request

Under the new Right to Access, any customer can ask to see their data, how it's being processed, where and for what purpose. As a business, you're obligated to provide customers with a copy of their personal data in an electronic format. Start reviewing how you access and pull customer data, and think about processes that can make dealing with these requests easier.

## Create processes for permanently deleting individual data

GDPR gives customers the right to request that you delete their personal data. As part of this process, you also have to make sure you're not passing their data on to third parties (e.g. automated email tools, social networks, etc.). Keep in mind that if customers withdraw consent for you to use their data, you must comply by going through this same process.

## Prepare for data breaches

Hopefully you never experience a data breach, but if you do, GDPR requires that you notify all affected customers within 72 hours. Make sure you have messages drafted and systems in place to move quickly if a breach occurs.

## Where to read the regulation

If you're preparing your business for GDPR, you might want to take the time to look through it. The actual language of GDPR is straightforward, although there is quite a lot to it. You can find

the entire regulation here or the chapter summaries here.

### Questions for your service providers about GDPR compliance

## Questions for your service providers about GDPR compliance

Most small businesses use service providers to process data. Point of Sale systems, cloud-based data storage, payroll processing and automated emailing services are all examples of data processors that many small businesses use. These service providers must be GDPR compliant by May 25, 2018. If they aren't compliant, and you continue to use them, you'll effectually be noncompliant.

To give you peace of mind, ask your service providers about their readiness for the upcoming implementation of GDPR. We've compiled a list of some of the most important questions to ask below.

### Data controller vs. data processor

Whether you are a data controller or a data processor, there are responsibilities unique to each role. GDPR defines these roles in the following ways:

- Data Controller is 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."
- Data Processor is the "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

A local restaurant that collects names, addresses, emails or phone numbers is a data controller. If that restaurant uses an email automation tool to contact those people about offers or specials, the email tool is the data processor.

Article 24 of the GDPR states that it is the responsibility of the data controller to ensure that data is processed in accordance with the regulation – including the scope, context and purpose of the processing. Meaning, as a controller, it's your responsibility to ensure that the data processing services you use are processing data legally.

### Is my data secure?

Service providers should encrypt data whenever possible, including when it rests in cloud storage or on servers. You should also ask who has access to your data, and if the processor runs frequent penetration and other security tests.

### Who has access to my data?

Your service providers might also use their own service providers for certain tasks. Any organisation that handles EU citizen data must comply with GDPR, so those third-party companies aren't exempt. If any of these organisations use data for purposes other than those the individual has explicitly given consent for, they are in violation of GDPR.

### How easy is it for you to delete my data?

The GDPR includes the right to erasure, also called the right to be forgotten. The concept has existed in the EU since the 1990s, but now it is a fundamental data right protected by the new law. Upon the request of the individual, organisations must be able to delete all data belonging to an individual. There are, however, several conditions in which the organisation might retain that data, such as financial records.

### What steps are you taking to ensure GDPR compliance?

If you simply need to know whether or not a service provider will be compliant– just ask. Data processors should be prepared to answer this question, and any defensive or evasive language about it should trigger warnings that they may not be prepared.

The bottom line is that the responsibility of ensuring GDPR compliance from service providers is shouldered squarely on the data controller. Approach the companies you rely on for services and ask questions.

### Consequences of non-compliance with GDPR

## Consequences of non-compliance with GDPR

On May 25, 2018, the General Data Protection Regulation (GDPR) comes into effect. It will impact businesses on a global scale, and the fines for non-compliance are severe. GDPR bolsters and consolidates previous data protection laws, while at the same time imposing hefty fees for non-compliance.

## Who enforces GDPR?

Each EU member state must designate at least one supervisory authority, and each of those authorities must also cooperate with one another on GDPR related activities. UK citizens will still have the same data protection rights as EU citizens post-Brexit. That means UK businesses should prepare to fully comply with GDPR by May 25th.

Chapter 6 of the GDPR explains the role and scope of each state's authority. Those authorities are "responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union."

Meaning, each state's authority is responsible for determining and applying non-compliance fines. They are encouraged to make the fines effective, proportionate to the offence and hefty enough to dissuade future offences.

## Guidelines for prosecution

Article 83 of the GDPR details how fines will be applied and how steep those fines are.

The authorities in each member state will use the fine guidelines GDPR has outlined. That means the authorities should take into account the specific type of offence, the severity and impact of the offence, and the amount of time over which the offence was committed. The scope and purpose of the data processing will be taken into account, as well as how many individuals were affected and how much the offence negatively impacted their lives.

The authorities will also consider if action was taken by either the data controller or the data processor to prevent harm or damage to individuals. They will take into account how responsible the data processor and controller were, based on the technical and organisational compliance with GDPR.

## Maximum GDPR fines

There are three main ways you can be non-compliant, with varying degrees of fines.

## Failure to meet obligations

The first category of infringement is listed as failure to meet obligations. The failure can be made by the data controller or the data processor.

Many of the responsibilities for each organisation is listed in Articles 25 through 39. Data breach notifications, verification of consent for use and processing, notification of identification, necessity of use, appointment of a Data Protection Officer (DPO) and a few other requirements are on the shoulders of the data controller and data processor.

Each infringement of the first category can be subject to an administrative fine of up to €10M, or up to 2% of the offending organisation's total worldwide annual turnover of the preceding fiscal year, whichever is higher.

## Mishandling EU citizen's data

The second category of non-compliance is about handling personal data. The right to erasure, also called the right to be forgotten, is the ability of EU citizens to request the erasure of non-essential data held. There is also the right of access, the requirement for transparency and the right to portability.

An infringement on those rights is weighed based on the same criteria listed before, but carries a steeper fine than the first category. The administrative fine can be up to €20M or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

## Non-cooperation with authorities

If GDPR authorities ask an organisation to stop data processing or collection and they continue to do so, they can be slapped with a hefty fine of €20M or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

## A GDPR HR checklist

These fines above not only apply to collecting and processing customer data, they also apply to your employees' data. Don't neglect this aspect of GDPR compliance! Use the steps below to start taking inventory of your HR processes.

1. Do you anonymise employee data or hiring data whenever possible?
2. Do you use a secure tool to store employee contracts?
3. Does your employment contract include a section on data training and data protection?

4. Can you easily delete an employee's data after they leave your company?
5. Do your employees know how you use their personal data?
6. Are all systems you use to store employee data GDPR compliant (i.e. payroll software, HR management, scheduling systems, etc.)?
7. Do you have a legitimate reason for collecting all the employee data that you do?
8. Can your employees easily edit their data?
9. Does your job application process comply with GDPR (i.e. asks only for necessary data, specifies for how long you will keep the data and notes other data that will be used in the screening process)?
10. Do you collect sensitive data like sexual orientation, gender, etc.?

If you can't answer any of the questions above or if you know you aren't compliant, then you need seriously to consider how you manage your employee data processes. Start by using a secure tool to manage your HR processes and check with your current service providers to see if they're compliant.

### Planday's GDPR compliance

## Planday's GDPR compliance

Everyone at Planday takes the security of our product very seriously. Our customers trust us with their data, and protecting that is central to running our business and helping our customers run theirs.

Planday has long partnered with data privacy specialists and legal advisors on an ongoing basis to ensure continuous compliance with GDPR and other worldwide data privacy regulations. Additionally, we're actively working with customers to fully understand their data processing and privacy needs.

The Planday executive team is committed to Planday's compliance with the General Data Protection Regulation.

Our compliance will build on the already safe and secure product we have now– ensuring your data and the data of your employees is as secure as possible. Planday complies with national data protection laws in all our markets, and we're a certified CyberEssentials holder, which is a UK government-backed cyber protection scheme.We're also registered with the Information Commissioner's Office (ICO) and Datatilsynet (the Danish data protection supervisory body).

Planday not only provides a secure solution for you, it also helps you become GDPR compliant by ensuring your employee's data is fully protected.

Below are the steps we're taking to ensure we're GDPR compliant.

## Risk profile

We haven't left GDPR compliance as an afterthought. In fact, we've been working towards GDPR compliance since November 2017, when we first ran a risk assessment on the type of data we process and store. Planday does not process sensitive data on a large scale, nor do we systematically monitor individuals based on personal data or use automated profiling.

## Planday system compliance

GDPR is not a one-off project, but an ongoing initiative that's part of Planday's continuous improvement model and enterprise risk management. We continuously strive to improve our incident management framework and continuous improvement register.

## Access control

All access to customer data is protected by roles and permissions within the Planday system. Planday employees can only access data on a need-to-know basis, and according to "the principle of least privilege," which means Planday employees have the minimal level of access to data in order to do their job.

We'll also help our customers become GDPR compliant by ensuring roles created in the system don't accidentally compromise data security.

## Data anonymisation and pseudonymisation

GDPR requires that certain data be either anonymised or pseudonymised. We know these are technical and complex terms, so if you have questions about what they mean, we recommend reading this article.

We use obfuscation as a way to anonymise data. Personal information like bank account details and personal identification numbers will be obfuscated– meaning only the last few digits will be shown (e.g. **** 1234).

## Data retention

Planday's data retention policy adheres to regulatory requirements. If you want more details on this, please contact us at support@planday.com

## Compliant third party systems

We only use third party systems that are compliant with GDPR.

## Encrypted data

Our customers' data is encrypted from end-to-end. This means when you enter information in the app, your data is sent to an https web processor, then stored in a database. Your information is encrypted throughout that journey, so it can't be read at any point.

## Secure passwords and verification

Only you can see your password, so even users with the highest admin access can't see other users' passwords. Your password will always be encrypted in the Planday system and database.

We require users to verify their email and use a secure password. We will also require all existing users to update their passwords and verify their email.

## Removing end user data

End user data is subject to our end user licence, as well as our retention schedule. The removal of end user data from customer portals is by request, and subject to a review by Planday and the portal's admins. End user data that is no longer relevant or required will be anonymised by removing any personal data.

## Planday business compliance

GDPR is a part of our enterprise risk management, meaning we think about GDPR compliance as part of the methods and processes we use to manage risks and achieve our objectives as a company.

## DPA

As a part of this compliance, Planday only processes data as per our Data Processing Agreement. All the data we process is protected in our infrastructure and SaaS systems– meaning the data we process never leaves a secure system.

When we process and access data, it's always with consent– whether it's in accordance with our Data Processing Agreement or with explicit customer consent. That ensures we fulfill our legal obligation to our customers to protect their data at all times.

## Planday employee access to data

Additionally, all access to customer data is protected by roles and permissions within the Planday system. Planday employees can only access data on a need-to-know basis, and according to "the principle of least privilege," which means Planday employees have the minimal level of access to data in order to do their job.

All access to customer data within the Planday product is via consent only. For example, when a Customer Success team member needs to access a customer's Planday account, the customer must give permission for the CS team member to access that data.

We require all our employees to complete data protection training, with an emphasis on how data protection relates to GDPR. Employees are routinely trained on new processes and procedures, and retrained on any subsequent changes.

Additionally, we require that each department document any process that relates to the processing of personal data. To protect our system against internal abuse, we also ensure Planday employees are given the minimum access to data required to carry out their role.

## Data breach management

GDPR requires that companies inform users if there is a data breach within 72 hours of discovering it. We have all the processes in place to ensure this is possible and easy to execute.

## Consent

One of the biggest changes in GDPR is how companies get consent from customers for using their personal data. We've updated our process for getting customers consent and have

informed customers how their data will be processed when using Planday. We will also ensure that only necessary data is collected in the first place.

### Risk management

Planday operates using a framework called continuous improvement model, which allows us to fluidly make changes to policy, process and procedure to combat any incoming risks.

### DPO

GDPR requires that some companies have a Data Protection Officer (DPO). Planday's DPO is responsible for the following:

- Educating employees on why GDPR compliance is important
- Training staff involved in data processing
- Auditing our systems to ensure compliance and addressing problem areas proactively
- Serving as the point of contact for GDPR authorities
- Maintaining data processing records, which must be turned over to customers if asked

### Additional security procedures

All customer data is encrypted and backed up to a secure facility. We also use antivirus or malware protection on all machines at Planday. All machines used for software development, or those that come in contact with sensitive data, use encrypted disks.

### We take customer trust seriously

Customer trust is the foundation of our product and our business– without it, we can't provide our customers with the solutions they need to better run their businesses. That's why data protection and privacy is something we've prioritised since the founding of Planday, and it's something we'll continue to prioritise with our Information Security Management System and compliance to various data privacy laws, such as GDPR.

### How Planday supports your GDPR compliance

## How Planday supports your GDPR compliance

We've had questions from customers lately about whether or not Planday is GDPR compliant. The answer? Yes.

The Planday executive team ensured Planday's compliance with the General Data Protection Regulation by May 25, 2018.
We understand that when it comes to compliance, you probably have some questions about which tool is the best choice. We think the answer to that is simple: Planday is the best choice for a secure employee scheduling solution, and we've outlined why below.

## Planday is already safe and secure

Our compliance will build on the already safe and secure product we have now– ensuring your data and the data of your employees is as secure as possible. Planday complies with national data protection laws in all our markets, and we're a certified CyberEssentials holder, which is a UK government-backed cyber protection scheme. We're also registered with the Information Commissioner's Office (ICO) and Datatilsynet (the Danish data protection supervisory body).

## You decide whether we can see sensitive data

Planday employees can only access data on a need-to-know basis, and according to "the principle of least privilege," which means Planday employees have the minimal level of access to data in order to do their job.

All access to customer data within the Planday product is via consent only. For example, when a Customer Success team member needs to access a customer's Planday account, the customer must give permission for the CS team member to access that data.

## Mandatory data protection training

Everyone who works at Planday has to undergo data protection and privacy training. Employees who can access sensitive customer data must go through even more extensive training on when it's appropriate to access that information, which they can only do after a customer has given them permission.

## We've long worked with top data privacy organisations

Planday has long partnered with data privacy specialists and legal advisors on an ongoing basis to ensure continuous compliance with GDPR and other worldwide data privacy

regulations. Additionally, we have a third party carry out extensive penetration tests and a security audit on a regular basis.

## Use our guidance on how to be GDPR compliant while using Planday

In preparation for GDPR, Planday can make the following recommendations to customers about data in the product:

- Review all permissions per roles that you have allocated to your users
- Review all the users, and de-activate any users that should not have access to your data
- Do not download personal data, including payroll data, from Planday onto work and personal devices
- Planday is not responsible for any data transferred from Planday into your own systems, such as data warehouses. Accordingly, please review security access, and data privacy for your own systems
- If sensitive data is entered into Planday, then please ensure that this data is treated appropriately. Planday is not liable for this sensitive data
- Review all the fields that are visible to your various users, and hide these when appropriate or desired

## Your data is safe with us

All customer data is encrypted and backed up to a secure facility. We also use antivirus or malware protection on all machines at Planday. All machines used for software development, or those that come in contact with sensitive data, use encrypted disks.

Customer data is encrypted from end-to-end. This means when you enter information in the app, your data is sent to an https web processor, then stored in a database. Your information will be encrypted throughout that journey, so it can't be read at any point.

Everyone at Planday, from our CEO to our newest hire, takes data protection very seriously. We've baked that into our culture by problem solving, developing and designing our product and processes with protection and security in mind. So, when you decide to sign up for Planday, know that you're in very safe hands.

## Choose your software providers carefully

In order for your business to be GDPR compliant, you must use service and software providers that are also compliant. The consequences on non-compliance are severe, so choosing

compliant providers is absolutely key to keeping your business financially afloat.

## FAQs about Planday's GDPR compliance

To make navigating GDPR easier for customers and partners, we've answered our most frequently asked questions below.

## What are Planday's GDPR contact details?

Name of company: Planday A/S

Address:
Kuglegårdsvej 7-9-11
building 181
1434 København K
Denmark

Data Protection Officer: Lasse Andersen, Director of Legal for Planday.

## Does Planday process sensitive data?

Planday does not systematically monitor individuals based on personal data, or use automated profiling of user data.

The app does have custom text fields in which sensitive data can be added by either the end user or their employer. These fields are configured by employees or their employers, who accept full liability for any sensitive data entered into these fields.  Any data entered into these fields will be processed in the same way as we process personal data.

## Does Planday subcontract any of processing activities to a third party?

Processing activities are only completed within our application / IT Infrastructure that is hosted in Denmark, as well as within any Software as a Service systems, such as our CRM and ERP systems.

## How will Planday ensure continued compliance to GDPR beyond 25 May 2018?

As we continue our ISO27001 certification, we will validate our compliance to GDPR and our commitment to information security.

## Does Planday have a Data Protection Officer?

Yes, our DPO is Lasse Andersen, Director of Legal for Planday.

## How does Planday promote data protection awareness?

Planday has various training programmes for employees about information security, including webinars from compliance specialists, internal communications and data privacy workshops.

## How is personal data stored?

Personal data is stored in our databases in our servers.

## Is any of Planday's data transferred outside the EEA?

Planday is a global company with legal entities in Europe, Asia and the USA. Employees can access customer data from our CRM and ERP systems in their office locations, and customers can access their data globally.

## Is Planday certified against ISO/IEC 27001 or part of a voluntary data protection scheme?

We are currently working towards ISO27000. We're registered with the UK-based Information Commissioner's Office (registration no. ZA259339), and Denmark-based Datatilsynets (registration no. 35107207). Planday is also a certified holder of CyberEssentials, a UK Government-backed cyber protection scheme.

## Does Planday have a documented response plan to address privacy incidents, unauthorised disclosure, unauthorised access or breach data?

Yes, Planday has an incident management process for all types of incidents, including data breaches. The plan aligns to industry standard. Please see our Status Page, for more details (we also highly recommend signing up for status updates).

## What security procedures does Planday use for protecting its systems against vulnerability and the data against accidental loss, destruction or damage?

Data in our SaaS systems is encrypted in transit and at rest. We also have role-based access control and two-factor authentication logins setup. Data in our product is encrypted in transit.

## How does Planday protect my personal data?

Planday takes security of personal data very seriously. Our risk management and security controls include:

- embedding data privacy by design into everything we do;
- consent and permission management;
- internal access control based on role and least privilege; all access is logged;
- risk management, business continuity, including disaster recover, backups, business impact assessments, risk registers and Data Protection Impact Assessments;
- data breach management: Planday will inform all users impacted of a data breach within 72 Hours;
- cryptography, crypto controls, key management;
- all data is backed-up;
- securing and alarming all of Planday's office facilities;
- asset management;
- network segregation, penetration testing, and a software development cycle
  data is encrypted in transit, and all backups are encrypted

## Is there any personal data that is used outside production environment that is not anonymized?

No

## What is Planday's process for any complaints relating to personal data or data breaches?

Planday's complaint handling policy ensures all end-user and customer complaints are appropriately handled, and complies with data protection laws and notification requirements.

If you have a compliant, please email support@planday.com and address the email to our DPO (Lasse Andersen, Director of Legal).

If you feel like your complaint hasn't been properly addressed after that, you have the right to file a complaint with a Supervisory Authority, such as the ICO or Datatilsynet.

## How does Planday handle my right to access my data? (GDPR's Right of Access)

Under Article 15 of the GDPR, an individual has the right to obtain their personal data that is processed by a controller. We are committed to upholding this right, and have a dedicated process in place for providing access to personal information. To access your data, please complete our Subject Access Request form.

## What about my right to be forgotten?

Please contact support@planday.com if you want to remove your data as an employee or any deactivated employee data as a customer. Please note that this request is subject to a review between Planday and the customer, and subject to both parties' retention schedule.

## Does Planday have any guidance for customers about how to be GDPR compliant while using Planday?

In preparation for GDPR, Planday can make the following recommendations to customers about data in the product:

- Review all permissions per roles that you have allocated to your users
- Review all the users, and de-activate any users that should not have access to your data
- Do not download personal data, including payroll data, from Planday onto work and personal devices
- Planday is not responsible for any data transferred from Planday into your own systems, such as data warehouses. Accordingly, please review security access, and data privacy for your own systems
- If sensitive data is entered into Planday, then please ensure that this data is treated appropriately. Planday is not liable for this sensitive data
- Review all the fields that are visible to your various users, and hide these when appropriate or desired

### How do I submit my data to Planday when working with the Activation Team?

All data that is sent to the Activation Team for uploading must be sent via a password protected Excel file. The password must be shared separately with the Activation Team, in a separate email. This is to ensure that the data is securely transferred between the customer and Planday. The Activation Team will not accept any data sent in an unsecured manner.

### How do I download data from Planday to process payroll?

You can download your data like you normally do. Once this data is transferred to your payroll system, Planday recommends that you delete this data from your computer. This should be checked and enforced from your side.

### Information Security Management System Policy

## Information Security Management System Policy

It is the policy of Planday to maintain an information security management system (ISMS) designed to meet the requirements of ISO 27001 in pursuit of its primary objectives, the purpose and the context of the organisation.

It is the policy of Planday to:

- make the details of our policy known to all other interested parties, including external once a non-disclosure agreement is signed and where appropriate, and to determine the need for communication and by what methods relevant to the business management system;
- comply with all legal requirements, codes of practice and all other requirements applicable to our activities; therefore, as a company, we are committed to satisfy applicable requirements related to information seclnurity and the continual improvement of the ISMS;
- provide all the resources of equipment, trained and competent staff and any other requirements to enable these objectives to be met;
- ensure that all employees are made aware of their individual obligations in respect of this information security policy;

- maintain a management system that will achieve these objectives and seek continual improvement in the effectiveness and performance of our management system based on “risk”.

This information security policy provides a framework for setting, monitoring, reviewing and achieving our objectives, programmes and targets.

To ensure the company maintains its awareness for continuous improvement, the business management system is regularly reviewed by the Executive team to ensure it remains appropriate and suitable to our business. The business management system is subject to both annual internal and external audits.

The scope of this policy relates to the technology and IT systems (computer systems) managed by the company to fulfil the company’s business of providing workforce management platform services. It also relates to, where appropriate, external risk sources including functions which are outsourced.