Overview - what is GDPR?

GDPR, or the General Data Protection Regulation, is an extension of our existing Data Protection Act, and comes into force as EU legislation on May 25th 2018, and will remain in force even after Brexit.

It's an evolution in how data is kept, used, and protected from misuse, and builds on existing best practices and common sense strategies. This new set of rules is a reaction to a number of recent high profile leaks and hacks of personal data from some of the largest corporations on the planet, but the wide ranging implications have resulted in actions that we all have to take, regardless of company size.

A Reminder About The Data Protection Act

The basic requirements and definitions of the DPA are still there in the new GDPR. Let's take a moment to remind ourselves what that means in terms of data ownership and processing.

The Data Controller is defined as the organisation "which, alone or jointly with others determines the purposes and means of the processing of personal data". That means you, as a Pinpointers Customer, you set the purpose for which the data is collected and analysed, making you the Data Controller.

The Data Processor is the organisation that processes personal data on behalf of the Data Controller. This applies to all cloud based service providers, from Google and Facebook to telematics companies such as Pinpointers.

So to summarise, you are the Data Controller and we are the Data Processor.

What Counts As Personal Data?

‘Personal data’ means data that relates to an identified or identifiable natural person (the “data subject”). As a customer, this will be the primary account holder, usually the person who signed up for the service in the first place, and as a fleet manager, there will be further data that will typically be associated with either ‘the driver’ or “the member of staff”.

An identifiable data subject is someone who can be identified, either directly from the data itself or indirectly by reference to an identifier like a name, an ID number, location data, or a vehicle registration name or number.

This is an important shift from previous definitions and is broad interpretation that can include data like IP addresses of a user’s personal device, their device ID, or their phone number, rather than just a vehicle number plate. This would include data derived from a telematics system that includes identifiers that can be linked to the driver of a telematics-enabled vehicle.

GDPR has very clear guidelines that state that personal data be:

- Processed lawfully, fairly and in a transparent manner
- Only collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes
- Adequate, relevant, and limited to what is necessary for achieving those purposes
- Accurate and kept up to date
- Stored no longer than necessary to achieve the purposes for which it was collected
- Properly secured against accidental loss, destruction or damage.

For clarity, Pinpointers can state that we:

- Only collect data for the purposes of providing a tracking and telematics service to you
- Store your tracking data for a default period of 12 months after which it is deleted
- Can delete some or all of your tracking at your request if you ask us to do so
- Delete all your personal tracking data when your contract comes to an end
- Retain only your basic company and primary contact details in case you take up a new contract at a later time
- Only offer password protected accounts on our system, no open access to data is granted unless you as the customer have explicitly asked us to, or you have done so by creating a Public Web Page
- Do not share any data for the purposes of marketing or analysis

What Personal Data Does Pinpointers Hold?

We hold two different types of personal data on your behalf.

Firstly we have your details as a customer of Pinpointers, so that's the primary account holder, company address details, email and phone number. We also hold basic details of any other people who have been given their own login to the Pinpointers portal, such as their name, email and optionally a phone number for SMS alerts.

Secondly, we hold all the tracking data from the devices installed in your vehicles or assets, or devices that are allocated to an individual such as a lone worker tracker, or from your mobile phone if you use any of our smartphone apps. This can include drivers names, and optionally their regular place of work or their home location, if you have added these as Placemarkers in the Pinpointers system.

Again, remember that you are the Data Controller and you have opted to give us your personal and company contact details so that we can enter into a contract with you, and you have chosen to track your vehicles and therefore by implication the movements of the individuals that drive them. We strongly advise that you have a clear statement in your company policies or contracts of employment that clarify the reasons for which you track your vehicles, and how you intend to use employees personal data in the event of any breach of trust or contract.

Customer Details and Direct Debit Bank Details

(Please note this is only applicable if you are a direct customer of Pinpointers, if you purchased the service through one of our approved resellers your financial information will be held by them)

We use a partner called First Capital Cashflow to manage the initial financial sign up to our service, and specifically, the declaration of a Direct Debit with bank details for the ad-hoc and regular payments for our goods and services. They are in turn a subsidiary of a company called BottomLine. They have issued their own GDPR compliance statement and have declared that they meet the requirements in full.

It is worth noting that they retain your personal details including your bank details in perpetuity, as the Direct Debit guarantee allows for an end customer to claim back payments unlimited by time and value.

Data Retention and Deletion

GDPR does not change the basic rules about data retention and deletion, but it is worth reiterating them here for clarity.

We retain historical tracking data for 12 months for each device that is in contract with us, in other words, where a paying contract is in place. The data is automatically deleted after this retention period.

You may request that we delete the historical data for any single device where the contract for that unit has expired or is cancelled, and we will fully delete that data within 30 days.

As the Data Controller, you might need to delete certain items in the Pinpointers System that could be considered personal data about an employee or ex-employee, such as Placemarkers at certain addresses, or Watches sending alerts to certain email addresses. We cannot be held responsible for these items, as we have no context with which to attach them to an individual or single tracking device.

We are compelled to keep certain personal data about you as a customer due to the need to keep seven years of financial data for the purposes of tax inspection or auditing. This data is limited to your company name, address, phone number, and the primary account holder name, email address and phone number.

In the event that your contract in its entirety with us is cancelled, we will delete all historical data and any data relating to secondary user accounts, such as name, email address, contact numbers, within 30 days. All Placemarkers, Watches, secondary user accounts and any other data that has been accrued as a result of providing a service to you will be deleted in full and will not be retrievable.

Data Transfers Outside The EU

When it comes to any cloud based service, we rarely stop to consider exactly where in the world our data is being stored.

The new GDPR sets very clear restrictions for the storage and processing of data outside of the EU or any EU approved ‘whitelisted’ countries, such as Switzerland. It's no surprise perhaps that the USA is not a whitelisted country. However there are provisions for the safe transmission and storage of data in the USA, which are covered by a framework called Privacy Shield.

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce

The Pinpointers service, which consists of a number of databases and web servers, are located in a secure data facility in the UK. We use a number of external services for certain tasks such as user authentication, using the Amazon Web Service (AWS). Our contract with Amazon stipulates that any cloud stored data is held in the UK or Ireland.

We also use a Google based service called Firebase, which assists us with the broadcasting of tracking data to the multiple web browsers that might be looking at the same data at the same time, it helps us to keep our service responsive and scalable. The Firebase service does store data on servers in the USA, but Google are fully compliant with the EU-US Privacy Shield Framework, which means the data is protected and safe.

Summary

In summary, Pinpointers takes the subject of data privacy and security very seriously indeed. We understand that we are holding and processing important and potentially sensitive data on your behalf. We have implemented a number of strategies to ensure compliance with the Data Protection Act, and now the GDPR.

Primary User, Secondary Users and Role Based Privacy

Each Pinpointers customer has a Primary User, and we need their approval to add any further secondary user accounts to the system. Each account can have full access to all data, or can be a restricted account with view only permissions. Data from tracking devices can only be viewed via user accounts created for that specific customer. It is not possible to view another customers data.

Secure HTTP

The Pinpointers web portal uses HTTPS - this is a secure encrypted end-to-end service that means none of the data held in the database can be intercepted and decoded as it makes its way across the internet to your web browser. If you were to view your account from a country outside the EU, no data is being stored or processed where you are, it is only being viewed via a secure web browser window.

Other Resources

The Information Commissioner's Office provides excellent guidance on the implications of the GDPR as well as all other aspects of data protection. See

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Disclaimer

This document represents our current understanding of the published GDPR which is still not a final standard, and is still subject to change. We have made best endeavors to interpret the requirements in regards to the service that we provide and the personal data that we hold. This document should not be relied upon as legal advice or how to determine how GDPR affects your own business and we recommend that you engage your own legal services to ensure you are fully compliant.