Plannr Data & GDPR Due Diligence Questions

GENERAL

Is your company aware of its responsibilities under the GDPR and is it ensuring compliance? Please describe what processes you are putting in place to ensure compliance.
Yes. The Directors of the business have been engaged in GDPR projects and fully understand our responsibilities in this area.

Name/ contact details of individual responsible for security/ data protection
Gareth Thompson
Director
Info@plannrcrm.com

1. SECURITY MEASURES TO PREVENT UNAUTHORISED OR UNLAWFUL PROCESSING

1.1. Is your firm certified under ISO27001 or accredited to any other security related standard/ code?

We are Cyber Essentials certified and our security processes and policies have been assessed independently. We intend to certify under ISO27001 in due course.

1.2. Are all staff informed of their responsibilities in keeping data secure in accordance with users' requirements? If so, how?

Yes. This forms part of induction training when employees start work with Plannr. Updates to security procedures, such as the introduction of GDPR is communicated in the form of training sessions with updates made to procedures as necessary.

1.3. Do such employees sign confidentiality undertakings?

Yes. This is part of our recruitment procedure and is included within the contract employees sign upon commencement of employment with Plannr.

1.4. How are your systems protected against newly discovered vulnerabilities or threats?

We subscribe to 3rd party services that regularly monitor our systems and compare them to all known vulnerabilities, any patches or other measures that are flagged are acted upon immediately.

1.5. What computer operating measures are in place to protect data?

Plannr offers two factor authentication as a standard feature for both the adviser access and client portal. Passwords of users are hashed and are never stored in plain text, and never visible to Plannr employees. Plannr has an optional inactivity-timeout of 20 minutes.

1.6. Where data is held in manual form, is it identified in any way as being confidential data belonging to users?

Plannr operates a paperless office with the aim to keep all documents in electronic format and encrypted. If any client data is printed it is transient and will be destroyed by shredding once the requirement to have a hardcopy has ended.

1.7. Will manual data be kept secure at all times?

Yes, it will not leave the office which is secured.

1.8. Will data only be processed in a secure area? What precautions are taken to ensure that non-authorised personnel cannot access the area / premises in which data is processed?

Yes. All client data is held in a central secure environment any Plannr staff engagement with customers is carried out on this secure environment and local copies of data are not produced. Computers are individually password protected, administrator Plannr accounts are password protected and passwords are keep in an encrypted password management tool. Plannr head office is secured via electronic door lock with PIN code entry and an intruder alarm system.

1.9. Do you maintain a record of any data protection training provided?

Yes, we record all staff training using a secure online service.

1.10. Describe what physical security measures you have in place for unauthorised access to any of your work space (i.e. key fob/ ID card)?

Our head office is secured via key fob / PIN code door entry as well as keyed entry.

1.11. What measures do you have in place to prevent staff from installing potentially malicious software?

Staff are prohibited from the use of USB devices from an outside source within the office. Firewalls and anti- virus systems are installed on all devices to prevent the spread of malicious software on the internal network.

1.12. How many members of staff will have access to our data?

Currently we have 14 staff members who have access to client records.

1.13. What measures are in place to prevent unauthorised access to data from outside hackers (e.g. firewalls) and to what extent is the adequacy of current precautions monitored?

Our servers are hosted on AWS and utilises their intrusion detection, firewall and other protection systems. We also use a 3rd party intrusion system that continually tries to exploit known vulnerabilities and reports back immediately of any findings with proposed remedies. We track Ip addresses and have a whitelist for administration and a full audit log of any and all activity internal and external.

1.14. Is there a formal policy on this?

Cyber essentials outline our policy on this and will be further enhanced as we approach ISO27001.

1.15. Do you enter into contracts with third parties for the provision of services which may involve intended or accidental access to user data e.g. software maintenance?

Yes, third party data providers and software integrations via our API. These are agree in contract with each customer before access is provided.

1.16. If so, do these contracts include conditions requiring confidentiality in respect of data and compliance with the security provision of the Data Protection Act?

Yes, as outlined in our Privacy Policy: https://Plannr.co.uk/privacy

1.17. How quickly can you react if a security vulnerability is identified in your product / service?

As soon we become aware of a security vulnerability we will act without delay to resolve the issue and suspend the service if necessary.

1.18. What are your timescales and costs for creating, suspending and deleting accounts?

Accounts can be created by an automated process and access is enabled after the compliant user security credentials are setup. Accounts can be suspended or delete immediately.

1.19. Is all communication in transit encrypted?

Yes., Plannr utilises SSL (HHTPS) encryptions for all sessions between browsers and our pplication. Plannr utilises an embedded secure messaging services that uses AES 256 encryption for communication with clients.

1.20. Do you encrypt all data 'at rest'?

Yes, Any data that we deem sensitive is encrypted at rest using the AES 256 encryption algorithm.

1.21. Will data be shared across other services you may offer?

Not currently and customers will need to provide authority to do so if we offer this in future.

1.22. Do you have an Access Control policy (i.e. only certain members of staff can access certain information)?

Not formally but only technical staff have access to administration tools, sales and admin staff are only able to access Plannr via the standard interfaces offered to customers.

1.23. To what extent are users' system-use logged and monitored?

A third party service is used to monitor access and will notify of abnormal activity. Plannr also logs all activity and logs are reviewed on request.

1.24. Are failed login attempts recorded and viewed on a regular basis?

Yes, we use a daily notification system to allow us to see if there have been cases of multiple logins to help protect accounts from logins from unknown IP addresses.

1.25. How do you protect information taken offsite?

Data only resides on our AWS servers local copies of this data are not permitted as part of normal working activity. If a local copy is required then this will only be held in an encrypted form on a Plannr machine that has password and 2FA to access the data, the data will be deleted once the specific activity has completed.

1.26. Do you have a procedure in place to ensure users are notified without delay of a data breach concerning the personal data of users and/ or clients?

Yes, in case of a data breach users will be notified within 24 hours of the discovery of the event.

1.27. What back-up systems are in place to prevent loss of data caused by system crashes?

Plannr utilises AWS enhanced backup service and has regular snapshots of the system taken. In the event of a system crash a new instance of Plannr can be built in less than an hour. In due course Plannr will be hosted across dual AWS datacentres and this will enable an instant switchover in case of a system crash.

2. DATA OWNERSHIP/ RETENTION AND DISPOSAL

2.1. Do you have a Data Retention policy?

We hold the data entered by our subscribers for the minimum period required by law and if required this could be an indefinite period.

3. LOSS, DESTRUCTION OF, OR DAMAGE TO DATA

3.1. Do you have a business continuity plan in place to deal with any interruptions to data processing/ breach of data protection legislation?

Yes. Plannr has formal plan in place.

4. DEALINGS WITH THE DATA PROTECTION/ INFORMATION COMMISSIONER

4.1. Are you aware whether you have breached the DPA 1998 in the last 3 years and if so was the breach reported to the affected data subjects/Information Commissioner?

No.

5. TRANSFER OF DATA

5.1. Will there be any circumstances in which data may be processed/ transferred to countries outside UK/ EEA?

Client data will not be processed / transferred to countries outside the UK. If a customer wishes to have an integration with a 3rd party that does, then a contract between them and 3rd party will need to be put in place.

5.2. Do you have safeguards in place at each location where data will be processed?

The physical datacentre where data is held by Plannr is constantly secured by AWS. Personal data is encrypted at rest using AES-256 and is only shown to authenticated users. When data is input, each webpage is secured via an EV SSL certificate.

6. Data ownership/ Retention and Disposal

6.1. Do you delete data completely if users delete it from the application?

Yes, if requested data is erased from the Plannr servers, unless we are subject to any legal requirement for us to retain the data.

7. Disposal of data

7.1. Is data removed from all equipment before that equipment is disposed of?

Yes. Any associated applications are removed and wiped by our web development team. Hard drives are removed and correctly disposed of.

7.2. How is data in manual form, disposed of?

Any print-outs are securely shredded by use of an industrial cross-cut shredder.

8. Changes to application/ services

8.1. Approximately, how often do you make upgrades to your application/ services?

Upgrades can take place daily but will typically be a weekly occurrence.

8.2. Will these upgrades impact use of your services?

Our upgrades are tested fully for compatibility before being deployed. They will not typically impact service and if they do we will notify all users accordingly.

8.3. How and when will you notify users about any scheduled maintenance?

As and when required we will notify via the embedded Plannr support capability and email notifications.

8.4. How easy is it to export data from your service when moving to a new service?

Plannr has a built in export capability to select section of the database or perform a full export.

8.5. Can users obtain a copy of their data in a usable format?

Yes, Plannr has a full export capability which gives a full .CSV output of all data stored in Plannr..

8.6. What happens to user data if use of Plannr is discontinued? Do you delete all data immediately and securely?

All data is kept secured in our databases and is deleted on request in accordance with our Terms of Business.

9. Loss, destruction of, or damage to data

9.1. How many copies of data are backed-up?

A real-time copy is kept on our infrastructure along with the AWS snapshot backup service which is near real-time..

9.2. How often are back-ups performed?

Snapshots are performed at multiple times during any 24 hour period.

9.3. What back- up systems are in place to prevent loss of data caused by events such as fire, flood and burglaries?

We utilise AWS backup services which take regular snapshots of server data. These are replicated on AWS UK infrastructure should we need to rebuild servers outside of the environment. It is our intention to implement a second datacenter in AWS Dublin to give complete resilience to these events in due course.

9.4. Is your computer equipment on which data is processed protected from power failure or electrical disturbances?

Yes. Al AWS servers are protected to the highest standards and meet Level 1 datacentre standards (see following question). All electronic appliances used in our office are subject to annual PAT tests, and all computers are powered by back-up power supplies providing a limited duration of power in the event of a power failure.

9.5. Are all areas in which data is processed suitably protected from damage by fire, flood or similar disasters?

Yes, we host at AWS and every AWS Region is designed and built to meet rigorous compliance standards including ISO 27001, ISO 9001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC3, PCI DSS Level 1, and many more. Our Cloud Compliance page includes information about these standards, along with those that are specific to the UK, including Cyber Essentials Plus.

9.6. How quickly will you be able to restore data, without alteration, from a back-up if you suffered a major data loss?

During normal working hours this should take less than one hour.

10. Availability

10.1. Do you have sufficient capacity to cope with a high demand from a small number of other users?

Yes, Plannr has scalability built into its code and architecture, this has been hooked into AWS scalable service that enables Plannr to dynamically scale resources as required.

10.2. Could the actions of other users impact on the quality of your service?

No, Plannr’s system design ensures that each instance of Plannr is protected against others.

10.3. Can you guarantee that users can access data and services whenever needed?

Plannr is intended as 24x7x365 service and we have hosted with AWS as they offer a 99.99% uptime. Outside of any scheduled maintenance we aim to offer Plannr to the same availability.