Wedlake Bell

Prohire Software Systems Limited ("Prohire")

White paper on Prohire GDPR compliance measures

11th May 2018

Contents

1. OVERVIEW

The purpose of this white paper is to explain the measures Prohire has implemented, in order to meet its obligations under the GDPR, and to assist its clients - independent hire companies - in meeting their GDPR obligations.

For the purpose of the GDPR, Prohire is a 'processor', and its hire business clients will be 'controllers' (both terms explained below). Controllers must only use processors that guarantee to implement measures that will enable the controller to comply with the GDPR.

This paper explains the measures Prohire has taken to facilitate its clients' compliance, and is intended as a means of providing documentary assurance to that end for the benefit of its clients.

2. LEGAL BACKGROUND

Processing 'personal data' - information about living individuals - is regulated by the GDPR. The GDPR replaces the Data Protection Directive 95/46/EC, and its UK implementing legislation the Data Protection Act 1998 ("DPA"), with effect from 25th May 2018. The GDPR incorporates the same fundamental concepts and principles as the Directive and the DPA, though is significantly more prescriptive for organisations, and introduces a number of new obligations. Essentially, the GDPR requires that individuals' personal data is processed fairly, and imposes a number of other requirements, such as the obligation to keep personal data secure.

The GDPR includes a number of sanctions for non-compliance, including fines of up to 4% worldwide annual turnover, or €20,000,000, whichever is greater. Organisations must be compliant with the GDPR from 25th May 2018. The Information Commissioner's Office ("**ICO**"), is the regulatory body responsible for enforcing the GDPR in the UK.

The GDPR draws the following distinction between 'controllers' and 'processors':

- **Controllers** decide the purposes and means of processing personal data. In relation to drivers' (or other hirers') personal data on the Prohire software platform, the independent car and van hire businesses that Prohire contracts with are controllers, and as such must comply with the GDPR.

- **Processors** process personal data on behalf of controllers, but do not take decisions. In relation to hire businesses' customers' (i.e. drivers') personal data, **Prohire is the processor**. This is because Prohire does not take decisions in relation to drivers' personal data, but instead hosts this information on a platform for use by the rental businesses it contracts with.

The GDPR imposes specific obligations upon controllers when they appoint processors. Controllers must comply with these obligations, or they risk breaching the security requirements of the GDPR.

The relevant provisions are Articles 28 and 32, which are explained below:

1. **Article 28**: Sets out the rules for controllers when appointing processors, and processors' obligations and responsibilities for handling personal data, which are as follows:

    - Controllers must only use processors that provide sufficient guarantees to implement appropriate technical and organisational measures so that processing meets the GDPR requirements.

    - Processors must be bound by a contract which sets out:
        - The subject matter and duration of the processing;
        - The nature and purpose of the processing;
        - The type of personal data;
            - The categories of data subjects; and
            - The obligations and rights of the controller.

2. **Article 32**: Imposes the obligation to implement a number of technical and organisational security measures upon processors and controllers, when processing personal data.

A summary of GDPR Articles 28 and 32 is attached as Appendix 1.

3. HOW PROHIRE COMPLIES

Prohire system

Prohire is a UK company that owns a software programme and associated database, used for independent car and van rental businesses (commercial and domestic use). As such, Prohire is a processor for the purposes of the GDPR.

Car and van rental businesses input their clients' personal data (drivers' details), into the system via a booking form and this auto-generates documentation for the rental business to lease their assets (e.g. the vehicles in their fleet). The system generates a number documents, including hiring order forms, quotations, confirmation emails, sales invoices and confirmation of payments.

Security measures

As a processor, Prohire must keep controllers' (i.e. hire businesses) personal data secure, and only process it in accordance with those hire businesses' instructions. Prohire ensures data security pursuant to the measures under Article 32 and compliance with the relevant provisions under Article 28 (highlighted in bold above) in the following ways:

- The database is stored in a locked rackspace onsite in a shared data centre which is only accessible to the technical director and certain members of the technical support team.
- The rackspace provider has access to the data centre but no access to the database.
- Technical security includes a dual firewall system (live and standby), password protection on the server, up to date Microsoft antivirus software updated daily and security patches.
- The live real-time database is secured by way of a replicated mirrored backup server onsite.
- Certain elements of the database are encrypted (the client record) and Prohire aims to fully encrypt this system.
- Physical access to the systems is limited by way of designated keycard access by the technology team only, separate from Prohire employee keycards.

GDPR Compliance

Prohire is aware of its obligations under the GDPR, and will assist its client with data subjects' requests if required (subject to its terms and conditions). Prohire has instructed external counsel (see below) to carry out a GDPR compliance review and provide a data protection impact assessment of the system, in addition to this paper.

4. WEDLAKE BELL

This paper has been prepared by Wedlake Bell LLP. Wedlake Bell is a full service law firm established in the City of London in 1780. It has a dedicated data protection team lead by James Castro-Edwards, who has been practicing in data protection since 2004, and wrote the text book on the General Data Protection Regulation for The Law Society, the professional association for solicitors in England & Wales. The team also includes Mick Gorrill, who was the former head of enforcement for the Information Commissioner's Office.

Prohire has instructed Wedlake Bell to carry out a review of its platform and its GDPR compliance generally.

5. CONCLUSION

The client (the data controller) must comply with Art.28 (1) and use only processors that provide sufficient guarantees. This paper constitutes documentary evidence of the guarantees provided by Prohire in order to assist it with its compliance obligations under the GDPR.

Prohire welcomes any questions and comments regarding its compliance with the GDPR.

James Castro-Edwards,
Partner, Wedlake Bell LLP
11th May 2018.

Appendix 2

Summary of Articles 28 & 32

Summary of Article 28

Article 28 sets out processors' obligations and responsibilities under the GDPR and they must:

- Only process personal data on the controller's documented instructions.
- Ensure that individuals authorised to process personal data are committed to confidentiality.
- **Take all measures required under Article 32 (security of processing). (Please see below).**
- Only engage another processor (e.g. a sub-processor) with the controller's written authorisation.
- Ensure another processor (e.g. a sub-processor) offers sufficient guarantees to implement appropriate technical and organisational measures so that processing meets GDPR requirements.
- Assist controllers by appropriate technical and organisational measures, to help controllers respond to requests for data subject rights.
- Assist controllers with their obligations under Articles 32-36 (security of personal data).
- Delete or return all personal data to the controller at the end of provision of services relating to processing, and delete existing copies unless required by law.
- **Make all necessary information available to the controller, to show compliance with processing obligations (as evidenced by this Whitepaper).**
- Allow for and contribute to audits conducted by the controller or the controller's auditor, including inspections.

Summary of Article 32

Article 32 sets out a processor's obligations and responsibilities in terms of data security.

The key point is that processors must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. (Please see below for more information).

These measures include:

- Pseudonymisation and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Article 32: Data security risks

In assessing the appropriate level of security, account shall be taken of risks to personal data which is shared, transferred, stored or otherwise processed.

Risks include:

- Accidental destruction
- Unlawful destruction
- Loss
- Alteration
- Unauthorised disclosure
- Unauthorised access