GDPR Data Protection Policy

Prepared by	James Blizzard, Technical Lead
Approved by	René Morency, Managing Director
Last updated	31st May 2019

In this policy “Browser” means one or all of Browser London Limited; and “worker” means a Browser temporary or permanent employee, or a person who while not employed by Browser provides services to Browser as an employee of an agency or as a consultant; and “customer” means an entity that has commissioned a schedule of service with Browser London Limited.

Introduction

Browser holds certain information about individuals which is defined as Personal Data under the General Data Protection Regulation (“GDPR”). Browser recognises the importance of the correct and lawful treatment of Personal Data. For the purpose of the GDPR Act the data controller for Personal Data processed by Browser can be one, several or all of Browser.

Data Protection Principles

Browser fully endorses and adheres to the principles of GDPR. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of Personal Data. Workers and any others who obtain, handle, process, transport and store Personal Data for Browser must adhere to these principles. The principles are as follows;

Lawfulness, fairness and transparency

Browser will (in plain english) inform the subject what data processing will be actioned, and the purpose of processing. The data that is processed must match up with how it has been described. The processing of data must meet the level of compliance as outlined in GDPR.

Purpose limitations

Personal data will only be obtained for specified, explicit and legitimate purposes. The data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

Data minimisation

Data collected on a subject should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. No more than the minimum amount of data should be kept for specific processing.

Accuracy

Data must be accurate and where necessary kept up to date, baselining improves data protection and mitigates against identity theft. A rectification process and data management / archiving activities protocol should be in place for subject data.

Storage limitations

Personal data should be kept in a form which permits identification of data subjects for no longer than necessary. Therefore data that is no longer required for a set purpose should be removed.

Integrity and confidentiality

Data should be handled in a manner that ensures appropriate security and confidentiality of the personal data including protection against unlawful processing or accidental loss, destruction or damage.

Satisfaction of Principles

In order to meet the requirements of the principles, Browser will:

- Observe fully, and review the conditions regarding the processing and control of Personal Data.
- Collect and process appropriate Personal Data only to the extent that it is needed to fulfil operational or any legal requirements.
- Apply regular reviews to determine the length of time Personal Data is held and for what purpose.
- Take the appropriate technical and organisational security measures to safeguard Personal Data.
- Ensure that Personal Data is not transferred abroad without suitable safeguards.
- Review and update our data-mapping to highlight data controllers and data processors.

- Regularly review and update the documented processes to deal with data subject rights, this includes; individuals' requests to access, amend or delete their personal data or object to data processing within the new timeframes.
- Regularly review and update our data breach notification procedure to detect report and investigate a personal data breach.
- Ensure our Data Protection Impact Assessment process is in line with GDPR.
- Regularly review and update our compliance audits or reviews in order to identify and rectify issues.

Data protocol

Browser enforces the following protocol which includes the implementation and maintenance of a comprehensive information security program that details administrative, technical, and physical safeguards to ensure the confidentiality, security, integrity, and availability of Confidential Information and Data and to protect against unauthorised access, use, disclosure, alteration or destruction of Confidential Information and Data. The Information Security Program shall include, but not be limited to, the following safeguards where appropriate:

(a) Access Controls - policies, procedures, and physical and technical controls: (i) to limit physical access to its information systems and the facility or facilities in which they are housed to properly authorised persons; (ii) to ensure that all members of its workforce who require access to Confidential Information or Data have appropriately controlled access, and to prevent those workforce members and others who should not have access from obtaining access; (iii) to authenticate and permit access only to authorised individuals and to prevent members of its workforce from providing Confidential Information or Data unauthorised individuals; and (iv) to encrypt and decrypt Confidential Information and Data where appropriate;

(b) Security Awareness and Training - a security awareness and training program for members of Browser's workforce providing Services hereunder, which includes training on how to implement and comply with its Information Security Program;

(c) Security Incident Procedures - policies and procedures to detect, respond to, and otherwise address security incidents, including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into Confidential Information or Data or information systems relating thereto, and procedures to identify and respond to suspected or known security incidents, mitigate harmful effects of security incidents, and document security incidents and their outcomes;

(d) Contingency Planning - policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages

Confidential Information or Data (or systems containing Confidential Information or Data), including a data backup plan and a disaster recovery plan;

(e) Data Integrity - policies and procedures to ensure the confidentiality, integrity, and availability of Confidential Information and Data and protect it from disclosure, improper alteration, or destruction;

(f) Storage and Transmission Security - technical security measures to guard against unauthorised access to Confidential Information and Data that is being transmitted over an electronic communications network, which may include a mechanism to encrypt Confidential Information and Data in electronic form while in transit over public networks or systems to which unauthorized individuals may have access;

(g) Testing - Regular testing of the key controls, systems and procedures of the Information Security Program to ensure that they are properly implemented and effective in addressing the threats and risks identified. Tests should be conducted or reviewed in accordance with its internal policies and procedures by internal auditors, independent third parties or staff independent of those that develop or maintain the security programs.

Data processing and data control

For Browser

Browser may process and control data related to any business or other activity carried out by Browser, or deciding whether to accept any person as a customer or supplier, or for retaining records of purchases, sales or other transactions for the purpose of ensuring that the requisite payments and deliveries are made or services provided by Browser or to Browser in respect of those transactions, or for the purpose of making financial or management forecasts to assist Browser in the conduct of any such business or activity.

For workers

Browser may act as “data processor” and data controller” disclosing workers’ personal information with organisations which provide administration and management services. In this scenario Browser will only disclose workers’ information to Browser’s service providers and agents for these purposes.

Browser may disclose workers’ personal information to third parties in the event that Browser sells or buys any business or assets, in which case Browser may disclose workers’ Personal Data to the prospective seller or buyer of such business or assets. Or, if Browser is under a duty to disclose or share workers’ Personal Data in order to comply with any legal obligation.

For customers

Browser may act as “data processor” only on instructions from the customer as “data controller” in relation to the processing of “personal data” carried out on behalf of the customer and shall take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction.

Depending on the services that have been provided, Browser may process data such as name, email address, postal address, telephone number and financial details, where they received the data from, when they received the data, and who they share the data with.

Browser may disclose customer data to third parties if the data is required to provide a service that has been requested and authorised by a customer for the provision of services. Or, if Browser is under a duty to disclose or share customer data in order to comply with any legal obligation.

Using data

The data we collect allows our business, our workers, and customers’ services to operate. Both custom and 3rd party components may be used as part of the services provided. These services may include: communication, document sharing, support, payments, marketing, and analytics. In order to operate and provide a service to our customers we may use the following 3rd party software:

To provide a service

- Amazon Web Services, for hosting and storage of data.
- Pusher, to provide chat services.
- Sendgrid, Postmark, and Mandrill to send emails.
- Google Analytics and Hotjar, to track user behaviour.
- BugSnag, to monitor bugs in our software.

To operate our business

- Xero, for accounting and billing.
- Nutshell, for Customer Relationship Management.
- Google, for email, and contractual or planning information.
- Slack, for internal communications.
- Freshdesk and Intercom, for Customer Support.
- Hiscox insurance.

We do not provide data to advertising agencies, or to other parties for similar, unconnected purposes.

Accessing data

GDPR gives all subjects including workers and customers the right to access information held about each of them. We have created a support line for all customers should they wish access their personal data, requests can be made by contacting Browser on datarequest@browsergroup.com, requests will be subject to our vetting service to ensure that the request is legitimate. Once approved data will be supplied within 28 days of a request and supplied in a common format such as a CSV to allow for transit and accessibility. Any access request may be subject to a fee to meet Browser's costs in providing a data subject/worker/customer with details of the information Browser holds about that data subject/worker/customer.

Processing jurisdiction

We use Amazon Web Services (AWS) and a number of component services and providers in order for some of our customer's services to operate. The majority of our processing is carried out on servers that are located in the European Economic Area (EEA). At the request of a customer, we may use other carefully chosen suppliers and providers to perform other discrete tasks which may result in data being transferred outside of the EEA.

In handling data, we follow best practices which include:

- Using encryption to communicate between users and ourselves.
- Restricting and logging those who have access to the data we hold.
- Not moving data from production to test environments.

Data security and monitoring

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage and that both access and disclosure must be restricted. All workers are responsible for ensuring that any Personal Data which they hold is kept securely; Personal data is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Customers shall only access the Data in any way such that they cannot and do not see any other data hosted or managed by Browser to maintain the confidentiality of the data hosted or managed. Browser shall as soon as practicable inform the Customer of any notice or communication concerning data protection legal obligations received from any person (including any data subject or caller) or any regulatory authority (including the UK's Information Commissioner) concerning the provision of the

Service to the Customer and co-operate fully (at the Customer's cost) with the Customer in relation to all relevant matters concerning data protection requirements in connection with the Service.

Both workers and customers must regularly check that any Personal Data that they provide to Browser is accurate and up to date, and inform Browser of any changes to information which they have provided, e.g. changes of address; If, as part of their responsibilities, Browser workers collect information about other people, they must comply with this Policy.

Retaining personal data

The data we process and control on behalf of our customers' are retained for as long as it is required for a service to be provided, as the data allows our customers' services to operate.

The data we collect on behalf of Browser is held to up to a maximum of six years from the date it was submitted. The data is reviewed on an annual basis and action taken should it be required. In order to operate and provide a service to our customers we may use the following 3rd party software:

For marketing purposes:

- Nutshell, for Customer Relationship Management.
- MailChimp, for newsletter services.
- Google Analytics, for campaign tracking.
- Hotjar, for campaign tracking.