GP Planning Ltd: Data Protection Statement

Context & Introduction

Introduction

GP Planning Ltd ("GPP") need to gather and use certain information about companies and on rare occasions, about individuals.

This can include clients, suppliers, consultants, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This Statement describes how Personally Identifiable Information (PII) (i.e. any data that could identify a specific individual) and other less sensitive data types such as business contacts and invoice information, must be collected, handled and stored to meet the Company's data protection standards and to comply with the law.

A data audit detailing the types of information held by GPP, its storage, usage, transfer and disposal methods, has been carried out and is appended to this document. This Statement and the data audit are live documents that will be updated on a quarterly basis.

Why this Statement exists

This Data Protection Statement ensures GPP:

- Complies with the General Data Protection Regulation 2018 (Data Protection Act 1998 now superseded) and follows good practice;
- Protects the rights of staff, clients and other data sources;
- Is open about how it stores, processes and disposes of data, and
- Protects itself and those whose data we handle, from the risks of bad practice or in the worst case a data breach.

General Data Protection Regulation 2018 (Previously Data Protection Act 1998)

The General Data Protection Regulation 2018 (GDPR) describes how organisations, including GPP, must collect, handle and store all information, particularly PII. This EU law replaces the Data Protection Act 1998 in May 2018.

The Regulation applies regardless of whether data is stored electronically, on paper or on other materials.

To comply with GDPR, all data held about companies and PII must be collected and used fairly, stored safely and not disclosed unlawfully. GDPR also gives individuals greater control over their own personal data.

GDPR has six areas of data protection principles; they are referred to as the Privacy Principles. They are:

1. You must have a lawful reason for collecting personal data and must do it in a fair and transparent way.
2. You must only use the data for the reason it is initially obtained.
3. You must not collect any more data than is necessary.
4. It has to be accurate and there must be mechanisms in place to keep it up to date.
5. You cannot keep it any longer than needed.
6. You must protect the personal data.

Furthermore, these principles are supported by a further overarching principle – Accountability. This means that GPP must not only do the right thing with the data, but must also show that all the correct measures are in place to demonstrate how compliance is achieved. A data audit forms part of this Statement and demonstrates GPP's compliance and how it is achieved. This are appended to this Statement all of which can be found on our website and within the electronic Company Policies file.

People, Risks and Responsibilities (The Statement Scope)

This Statement applies to:

- All locations where work is carried out by GPP, including when working from home and when travelling;
- All staff of GPP, and
- All contractors, suppliers and other people working on behalf of GPP.

It applies to all data that the company holds relating to PII but also to any other sensitive data held about companies, suppliers, consultants and other data sources.

After assessment, using a data flow audit, it considered that GPP's processing of data will not result in a high risk to the rights and freedoms of individuals. Despite this, GPP takes its accountability and responsibility very seriously. A copy of this Statement can be found on our website, in staff handbooks and electronically. All staff will be regularly trained on data protection and privacy.

Data protection risks

This Statement helps to protect GPP and those whose data we handle from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them or their company.
- Right to erasure of data. Under the GDPR, a data subject has the right to ask for their data to be removed from ALL systems. It is therefore of paramount importance that the data flow audit is used as a working document to record where and how all data is collected, stored, transferred and disposed of. This can be found at the end of this document.
- Reputational damage. For instance, the company and individual could suffer if hackers successfully gained access to sensitive data, such as PII held about staff or project correspondence between employees and clients.

Responsibilities

Everyone who works for or with GPP has some responsibility for ensuring data is collected, stored and handled appropriately.

Each staff member that handles PII and other sensitive data must ensure that it is handled and processed in line with this Statement and GDPR privacy principles.

However, the following people have key areas of responsibility:

The Directors are ultimately responsible for ensuring that GPP meets its legal obligations.

- The Finance and Office Administrator is responsible for the following;
    - Assisting to keep the Directors updated about data protection responsibilities risks and issues;
    - Reviewing all data protection procedures and related policies;
    - Arranging data protection training and advice for the people covered by this Statement;
    - Handling data protection questions from staff and anyone else covered by the Statement;
    - Dealing with requests from individuals to see the data GPP holds about them (also called 'subject access requests');
    - Ensuring all systems, services and equipment used for storing data, meet acceptable security standards;
    - Checking and advising on any contracts or agreements with third parties that may handle the Company's sensitive data, and
    - Evaluating any third-party services the Company is considering using to store or process data. For instance, cloud computing services, including accountancy software.

- The Directors, Maureen Darrie & Christian Smith, are responsible for :
    - Overseeing all of the above with the Finance and Office Administrator (since GPP does not have an appointed data protection officer);
    - Approving any data protection statements attached to communications such as emails and letters;
    - Addressing any data protection queries from journalists or media outlets like newspapers;
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles, and
    - Overseeing any data protection and privacy policy training, data disposal and erasure requests

General Staff Guidelines

- The only people able to access data covered by this Statement should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from the Directors who will determine if the data can be released.
- GPP will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the Company or externally.
- Data should be regularly reviewed (quarterly) and updated if it is found to be out of date. If no longer required it should be deleted and disposed of.
- Employees should request help from a Director or the Finance and Administration Officer if they are unsure about any aspect of data protection

Data Storage

These rules describe how and where data should be safely stored.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the papers holding PII data should be kept in a locked drawer or filing cabinet. Documents containing sensitive data should be filed away appropriately and safely.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, for instance on a printer.
- Data printouts of PII or sensitive data should be shredded and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- PII data will be protected by strong passwords that are changed regularly and never shared between employees.
- Sensitive data should also be password protected.
- PII data will not generally be stored on removable media (like CD, DVD, portable drive). Where this is necessary these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and services and should only be uploaded to an approved cloud computing services.
- The back -up servers containing data should be sited in a secure location away from the main office space.
- Data will be backed up frequently and tested regularly.
- Should sensitive data be saved on to laptops or other mobile devices, this should be password protected and then deleted once no longer needed. PII data should not be saved onto mobile devices other than laptops used for business purposes.
- All servers and computers containing data should be protected by an approved security software and firewall.

When data is stored on **cloud based applications** such as Mailchimp, Xero and the pension administration dashboard, these applications will only be used once they have been assessed by the Finance and Office Administrator and the Directors to ensure their appropriateness in meeting acceptable security standards.

- Cloud based data storage accounts will be accessed by a restricted number of employees and will be protected by strong passwords that are changed regularly.
- After an initial opt in request sent prior to 25 May 2018, those on GPP's Mailchimp mailing list will be reminded during each contact that they can opt out and remove their data from the mailing list or update their contact preferences.

Data Use

Besides the PII data that the company holds for employees in order to carry out HR functions such as payroll and pension administration, it is rare that GPP collects or makes use of PII data. As stated within the Statement Scope, it is considered that GPP's processing of data will not result in a high risk to the rights and freedoms of individuals.

It is worth being aware however, that it is when this data type is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended, particularly during invoicing, payroll and pension administration.
- PII data should not be shared informally. In particular, it should not be sent by email to unknown recipients, as this form of communication is rarely secure. When PII data needs to be shared, with the company accountants for instance, the recipient should be expecting the data to be sent within a certain time frame and able to confirm receipt.
- PII and sensitive data should never be transferred outside of the European Economic Area.

The data most used by GPP is that of client, consultant and supplier contact details and other data for use in carrying out the purpose of the business, contacting consultants and invoicing clients. It contains PII in the form of individual contacts employed by the instructing client company. The data does not contain home addresses and other personal information, unless the business is that of a sole trader who chooses to use their PII such as their name and address as their registered business, in which case, the information is in the public domain and therefore using it without anonymization is not a data breach.

During the normal course of business GPP needs to establish details of landowners for the purpose of serving appropriate notice of a forthcoming planning application. This is a legislative requirement and the details will be shown on publicly available application forms. Notwithstanding that, GPP will not retain the data in any other form than the Notice, Form and covering letter correspondence. Where it is necessary to obtain that information from a third party, GPP will confirm that it is necessary for a 'contractual requirement' and that the data will only be used and kept in the above manner.

Data Accuracy

The law requires GPP to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated.
- GPP will make it easy for data subjects to update the information GPP holds about them, if requested.
- Data should be updated as and when inaccuracies are discovered.

Subject Access Requests and 'Right to Be Forgotten'

All individuals who are the subject of PII data held by GPP are entitled to:

- Ask what information the company holds about them and why;
- Ask how to gain access to it;
- Be informed how to keep it up to date, and
- Be informed how the Company is meeting its data protection obligations.

If an individual contacts the Company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to info@gpplanning.co.uk and marked 'GDPR Enquiry'. Individuals will be charged £10 per subject access request and GPP will aim to provide the relevant data within 14 days. The identity of anyone making a subject access request will be verified before any information is handed over.

Individuals also have a 'Right to be Forgotten', meaning that all PII data pertaining to that individual must be removed from all of our records. Such requests should be made in the same way as Subject Access Request and will be dealt with within 14 days. *

Disclosing Data for Other Reasons

In certain circumstances, GDPR allows PII data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, GPP will disclose requested data. However, the Directors will ensure the request is legitimate, with assistance from the Company's legal advisers where necessary.

Providing Information

GPP aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used, and
- How to exercise their rights.

To these ends, the Company has carried out a data audit, setting out how data relating to individuals is used by the company, this are appended to this statement.

Disposing of Data Securely

Data will not be held for longer than is necessary and will disposed of in an appropriate and secure manner.

Data relating to PAYE, maternity pay or statutory sick pay will only be kept for 3 years after an employee leaves GPP, as that is how long HMRC may be interested in the information for conducting reviews or audits.

Data such as employees' personal records, performance appraisals, employment contracts, etc. will be held for 6 years after they have left GPP. Under the GDPR, the condition for this processing period is GPP's legal obligation.

Sensitive data such as financial information, invoices, supplier contracts etc will be held for no-longer than 7 years for HMRC/accountancy purposes.

Closed or archived files pertaining to planning services will be retained for as long as is deemed necessary (decided upon on a case by case basis) however as far as is practicable PII will be removed from this stored data. Once no longer needed, all paper files and documents containing PII or sensitive data will be shredded and disposed of securely.

Electronic files will be deleted and removed from archive/recycle bins and the server memory upon request to our IT consultants Keith Withnall Associates.

* GPP has a supplementary in-house Privacy Policy that includes a Data Flow Audit and our detailed Right to be Forgotten and Subject Access Request procedures.

Latest version updated: 23/05/18

GPP Data Audit

Type of Data	PII collected is limited to: Names of individual contacts employed by clients and business contacts. Employee personal information.
Description of Data	Clients & Business Contacts: Individual contact name of those employed by client/business contact only. Employees: Name, addresses, bank details, insurance documents and drivers licence, CV and employment history.
Employee responsible	Directors and Finance and Office Administrator.
Date of consent to hold data	Date the terms of business are signed, this forms the contract between GPP and the client. If less instructions are given by email/telephone etc these will be the date of the implied contract, and are subject to the same privacy statement. Date of commencement of employment (data such as CV etc will have been provided prior to this but only upon the request of the potential employee).
Where the data is stored	• Client and business contacts PII is kept on paper and electronic files. These are kept securely within GPP's office which has restricted access to employees only (by use of security pass cards). Electronic files and data are backed up on a secure server. • Some paper files will be stored at our secure off site archive storage facility. Access is restricted to Directors only. • Personally Identifiable Information (PII) is kept on paper files. Staff files are in a locked cupboard (to which the Directors have the key). It is also kept in restricted access electronic files backed up on a secure server. Just the Directors and Finance and Office Administrator have access to these files. • This PII is also stored on the Royal London Pensions Administration system (Dashboard) which is password protected and has restricted access (one Director and Finance and Office Administrator only).
Source of the data	• Directly from the clients and business contact who instruct GPP. • First hand from the employee.

	• Company Accountants. Directors (whilst carrying out HR functions such as contract writing, reviews etc).
Purpose of the data	Clients & Business Contacts: Record individual contact and organisation's details for accounting and time recording, plus paper and electronic project files, in order that we can provide clients with our planning consultancy services. Employees: The company holds this data about employees in order to carry out HR functions such as payroll and pension administration
How the data is protected in its storage	See "Where the data is stored."
Usage restrictions	Client and Business Contacts: Only employees of GPP and in certain circumstances, we may need to discuss aspects of the business with others in order to carry out instructed work. Employees: Usage is restricted to Directors, Company accountants and the Finance and Office Administrator.
Usage rights	As above plus the data subject (i.e. individual contact / employee) who has the right to see all details held about them.
Usage frequency	On a daily basis.
Retention period	Client and Business Contacts: • Data will not be held for longer than is necessary to carry out the work, GPP's due diligence and to comply with the law. GPP will only keep the minimum amount of data needed. • Sensitive data such as financial information, invoices, supplier contracts etc will be held for no-longer than 7 years for HMRC/accountancy purposes. • Closed or archived files pertaining to planning services will be retained for as long as is deemed necessary (decided upon on a case by case basis) however as far as is practicable PII will be removed from this stored data. Once no longer needed, all paper files and documents containing PII or sensitive data will be shredded and disposed of securely. Employees: • Whilst in employment. • PII data relating to PAYE, maternity pay or statutory sick pay will only be kept of 3 years after an employee leaves GPP (HMRC period for conducting reviews or audits).

	• Data such as employees' personal records, performance appraisals, employment contracts, etc. will be held for 6 years after they have left GPP (legal obligation).
Comments	This is a working document that will be reviewed and assessed on a quarterly basis.

Latest version updated: 23/05/18