Pritchard Patent Product Company (2001) Limited
GDPR Data Protection Policy

Introduction

As we engage with people interested in our services, we need to collect and use information that relates to them.

We also need to collect and use information about the people who work with us, which includes employees, suppliers, consultants, contractors and other people that we have a relationship with.

This policy describes how we will collect, handle and store people's personal data to ensure that we meet our high data protection standards and to show to people that we comply with relevant legislation.

Why have we created this policy?

This policy ensures that Pritchard Patent Product Company (2001) Limited:

- **Complies** with data protection laws and follows good practice;
- **Upholds** the rights of its employees, customers and partners;
- **Is fair and transparent** in how it collects, processes and shares personal data; and
- **Protects** the individual personal data it holds, by reducing the likelihood of a data breach.

Data protection law

The General Data Protection Regulation (GDPR) sets out how organisations, including Pritchard Patent Product Company (2001) Limited, must collect, process and share personal data. These rules apply regardless of whether data is stored electronically, on paper, or using other materials/methods such as CCTV or other recordings such as call recordings, drones and dash cams.

Personal data or Personally Identifiable Information (PII) as it is known under the GDPR, is information that can be used on its own, or with other information to identify, contact, locate or identify a living person. Information can include but is not limited to:

- Name
- Email address
- Telephone number
- Postal address
- Date of birth

You should assume that whenever you handle personal data, it will involve some type of processing and therefore it must be carried out in accordance with the requirements of the GDPR. At least one of the following must apply to permit you to collect and process personal data:

1. **Legitimate Interests:** the processing of personal data is necessary for the company's legitimate interests unless there is good reason to protect the individual's personal data. The test is whether an individual would, or should, reasonably expect the processing to take place by the company

2. **Contract**: the processing is necessary for the performance of a contract with the individual, or to take steps to enter into a contract e.g. contracts of employment, reservation agreements
3. **Legal Obligation**: the processing is necessary for us to comply with the law (not including contractual obligations) e.g. undertaking Anti-money laundering checks for fraud prevention
4. **Vital Interests:** the processing is necessary to protect someone's life i.e. keeping next of kin information for health and safety purposes
5. **Consent:** we have obtained the individual's consent to process the personal data e.g. when sending out marketing campaigns

Pritchard Patent Product Company (2001) Limited must be responsible for and be able to demonstrate that personal data is:

1. Processed fairly and lawfully;
2. Obtained only for specific lawful purposes;
3. Adequate, relevant and not excessive;
4. Accurate and kept up-to-date;
5. Not held for any longer than necessary; and
6. Secure and protected.

People, Risks and Responsibilities

Who does this policy apply to?

- Pritchard Patent Product Company (2001) Limited Head Office;
- All brands of Pritchard Patent Product Company (2001) Limited;
- All divisions, branches and offices of Pritchard Patent Product Company (2001) Limited, whether permanent or temporary;
- All employees, regardless of work level;
- All contractors, suppliers and other people working on behalf of Pritchard Patent Product Company (2001) Limited;
- Any of our joint venture partnerships.

It applies to all personal data that the company holds, this includes:

- Customer information e.g. Prospects or those who have purchased our services, including family members;
- Employee details e.g. Health information, financial details, benefits and pensions
- The use of CCTV within our Offices to ensure we provide a safe and secure environment for all visitors to our premises and for the protection of our employees and property; and
- Recorded calls for training and quality purposes to and from our Customer Services and IT Service desk.

What are the risks involved?

This policy helps to protect Pritchard Patent Product Company (2001) Limited from some very real data security risks, including:

- **Breaches of confidentiality**

This could include information being given out inappropriately, sharing too much information or sharing information without consent or lawful basis.

- **Failing to be transparent**
  For instance, not telling individuals how their information will be used, using their information for different reasons to what they have been told and failing to inform individuals as to how they can exercise their rights.
- **Reputation damage**
  For example, the company could suffer if hackers successfully gained access to sensitive data or it was found to be breaching privacy principles.
- **Fines**
  The company could be fined up to €20 million, or 4% of global turnover, whichever is higher. Individuals could also bring a compensation claim against the company for any damages that they believe they have suffered.

The 'Data Protection Framework'

To ensure consistency in the way in which we handle personal data, Pritchard Patent Product Company (2001) Limited has put in place a Data Protection Framework, which includes policies, procedures, guidance and records.
It covers:

Our compliance processes and procedures
Employee awareness training ensures that teams are aware of data protection and its implications before choosing a particular route. Further details can be located within the Data Protection Chapter under the Pritchard Patent Product Company (2001) Limited Policies and Procedures Manual.

Privacy and Security by Design
Data protection is fundamental to our approach to any new business or initiative. As a result, we have integrated security and data protection into our operational processes. This means certain changes, risks and incidents trigger specific actions such as:

- Documenting our processing activity
- Data Protection Impact Assessments (DPIA); and
- Change Control

Privacy by Design
Privacy by Design is an approach to company initiatives, projects and IT system changes that promotes consideration of privacy and data protection compliance from the start. Undertaking this process will help us identify any potential problems from an early stage, considering risk and ensuring we put adequate measures in place to safeguard individual's personal data.

Data Privacy Impact Assessments (DPIA)
Data Processing Impact Assessments (DPIA) is a tool that we use to identify and reduce the privacy risks of any new or revised projects. A DPIA helps us to consider what data protection risks may occur if we undertake a particular project or partner with a new third-party supplier. The DPIA helps us to work through specific questions, which can reduce the risk of harm to individuals through the misuse of their personal information. It can also help us design more efficient and effective processes for handling personal data.

Change Control

If you are looking to:

- introduce a new internal system; or
- make changes to existing systems and processes; or
- share data with new partners

then these must be assessed and be approved via the following Change Control Boards:

- Data Protection Officer (DPO)
    - The DPO is the first tier responsible for taking a detailed holistic review of IT related changes. Primary objectives of the DPO are to review, in detail, company IT proposals and make recommendations to the Senior Management team as to whether projects should be initiated and implemented into the company.

- The Directors approve changes and investment in new systems and allocates resource to IT projects.

Governance

All employees should be aware of the structures in place, so that they can assure suppliers, identify risks, report breaches in security and handle requests for information.

Responsibilities

Everyone who works for or with Pritchard Patent Product Company (2001) Limited shares the responsibility of ensuring that data is collected, stored, processed and shared appropriately. Departments or functions that handle personal data must process it in line with this policy and the data protection principles. In addition to this, certain people and teams have specific areas of responsibility:

- **The Board of Directors**
  Ultimately responsible for ensuring that Pritchard Patent Product Company (2001) Limited meets its legal obligations.

- **The Data Protection Officer (DPO)**
  The person in this role is responsible for:
    - Keeping the Board updated about data protection responsibilities, risks and issues;
    - Reviewing all data protection procedures and related policies in line with an agreed schedule to ensure they remain up to date and effective;
    - Dealing with requests from individuals who want to see the data that Pritchard Patent Product Company (2001) Limited holds about them (Subject Access Requests);
    - Has responsibility to reporting any breaches to the ICO;
    - Handling data protection questions from employees and anyone else covered by this policy;
    - Checking and approving any contracts or agreements with 3rd parties that may handle personal data; and
    - Reviewing and signing-off Data Protection Impact Assessments.

- **Group IT**
  They are responsible for:

- Ensuring that all systems, services and equipment used for storing personal data meet acceptable security standards;
- Performing regular checks and scans to ensure security hardware and software is secure and fit for purpose; and
- Evaluating any 3rd party services the company is considering for the storage or processing of personal data.

- **Group Sales and Marketing**
  They are responsible for:
  - Approving any data protection statements in our customer communications, such as emails, letters and online;
  - Where necessary, working with other employees to ensure marketing initiatives abide by the data protection principles; and
  - Ensuring marketing databases are checked against our suppression files (email addresses not to be used by us) each time a marketing campaign is run.

- **HR**
  They are responsible for:
  - Ensuring the company holds employee data securely;
  - Obtaining consent for any sensitive categories of data the company wishes to use;
  - Has adequate measures in place between us and any external 3rd parties which process personal data on behalf of the company (e.g. pension providers); and
  - Arranging data protection training and awareness for the company.

- **Management at all levels**

  These individuals are at Department and functional level and are responsible for:
  - Ensuring fulfilment of the data protection provisions within their department or function;
  - Liaising with the Senior Management Team and DPO on responsibilities and controls;
  - Carry our local data destructions (paper stores etc);
  - Complete a Self-Audit each year on behalf of the division on active GDPR controls; and
  - Assist the division in ensuring that DPIAs are considered and carried out.

- **Senior Responsible Owner (SROs)**

  These are individuals who are responsible for:
  - Introducing new systems; and
  - Vetting our suppliers with whom we share personal data with.

General employee's guidelines

To ensure the objectives of this policy are met, we have outlined the steps we should take as a business to reduce the likelihood of a breach of information.

Necessary eyes only
The data covered by this policy should only be accessed by those who need to do so for work purposes. Data should never be shared informally. Personal data should not be disclosed to unauthorised people, either within the company or externally.

Time to train
Pritchard Patent Product Company (2001) Limited will provide training to all employees, so that you know what your responsibilities are when handling data.

Strong passwords
We must use strong passwords at all times and they should never be shared unless authorised by IT. Our baseline standard criteria for passwords should:

- Not contain your username or full name, or parts of your username or full name that exceed two consecutive characters;
- Be a minimum of 6 characters in length. There is no maximum length; and
- Contain a minimum of 1 character from three of the following four categories:
    1. English uppercase characters (A-Z)
    2. English lowercase characters (a-z)
    3. Base 10 digits (0-9)
    4. Non-alphabetic characters (e.g.!, £, #, %)

Ask for help
If you are unsure about any aspect of data protection, ask for help from your Line Manager or the DPO.

Data storage

The following rules describe how and where data should be safely stored:

When keeping paper records:

- **Keep data locked away:** When not required, paper files should be kept in a locked drawer or filing cabinet.
- **Keep it secure:** Paper and printouts must not be left where unauthorised people could see them (e.g. on a printer).
- **Shred when done:** Any printouts of personal data should be shredded and disposed of securely when no longer required.

When keeping electronic records:

- **Use strong passwords:** Data must be protected by strong passwords, see above, that are never shared.
- **Keep data locked away:** If data is stored on removable media (e.g. USB, DVD) these must be encrypted and kept locked away when not being used.
- **Use designated servers**: Data should only be stored on designated drives and servers and should only be uploaded to approved cloud computing services.
- **Use secure locations:** Servers containing personal data must be sited in a secure location, away from the general office space.
- **Back-up frequently**. Data backups must be tested in line with company standard backup procedures.
- **Keep it secure:** Never save data directly onto your laptop or other mobile devices.

When using data:

- **Secure your screen:** When working with personal data, ensure that you always lock the screen of your computer when unattended.

- **Keep it to yourself:** Personal data should not be shared informally. Care should be taken when sending emails which contain information that may harm an individual's right to privacy if disclosed to the wrong people – email is not a secure form communication.
- **Use encryption:** Data must be encrypted before it is transferred electronically.
- **Ask before sending:** Personal data should never be transferred outside the European Union without consulting the Data Protection Officer or a senior Director.
- **Keep it secure:** Never save copies of personal data to your own computer.
- **External storage solutions:** Any personal data must not be stored onto external storage solutions which are not managed by IT (i.e. personal Dropbox)

GDPR Data Map

To comply with the GDPR requirements, we will maintain a formal and accurate record of our data processing activities. The Data Map is will include:

- Information assets;
- Processing & activities;
- 3rd Parties (Partners);
- Data Transfers; and
- Risks and Controls.

Data accuracy

It is important that the data we process is accurate and, where necessary, kept up-to-date. In fact, the more important the information is, the greater the effort we should put into ensuring its accuracy.

Storing data
Data should be held in as few places as necessary. Employees should not create any unnecessary additional data sets.

Correcting data
Employees should take every opportunity to ensure data is up-to-date, for instance, by confirming a customer's details when they call. Be sure to update our systems as soon as you discover an inaccuracy.

Enabling amends
Pritchard Patent Product Company (2001) Limited make it easy for individuals to update the information held about them (e.g. via notification to HR and Payroll).

Requests for information

If individuals contact us to ask about the information we hold on them, it is called a 'subject access request'. All individuals that we hold information about are entitled to:

- Request to know what information Pritchard Patent Product Company (2001) Limited holds about them and why;
- Ask for a copy of the information we hold about them;
- Learn how to keep their data up-to-date;
- Learn how to object to processing;
- Find out how their data is being used; and

- Learn about the security safeguards we have in place to prevent the accidental or deliberate disclosure of their information.

Subject access requests are addressed in a separate policy.

Disclosing data for legal reasons

In certain circumstances, the GDPR requires personal data to be disclosed to law enforcement agencies without the consent of the individual concerned.

Under these circumstances, Pritchard Patent Product Company (2001) Limited will disclose the requested data. However, the Data Protection Officer must be informed first, so that they can confirm the request is legitimate and ensure that it is handled correctly.

In the interest of fairness

It's our aim to make sure that individuals understand when their data is being processed, how their data is being used and how to exercise their rights. To achieve this, we have written a GDPR Data Protection Policy and Cookies Policy, which sets out how personal data is used by the company(s). This is available on the Pritchard Patent Product Company (2001) Limited website.