POND GROUP LIMITED
DATA PROTECTION POLICY
MAY 2018

CONTEXT AND OVERVIEW

KEY DETAILS

Policy prepared by: Greg Gillies
Approved by Board / Management on: 17 May 2018

INTRODUCTION

Pond Group Ltd is a specialist risk and intelligence company with a global client base; the Company's expertise spans widely the aspects of risk and intelligence – with its main business including Intelligence, Protection and Investigation services.

Pond Group Ltd must comply with the European Union General Data Protection Regulation (GDPR) and other relevant legislation protecting privacy rights. As the Company is both Data Controller, and also Data Processor for certain activities, the scope of this policy applies to all processing of personal data by the Company.

These data protection laws require Pond Group Ltd to protect personal information and control how it is used in accordance with the legal rights of the data subjects
– the individuals whose personal data is held.

All data subjects are entitled to know

- Their rights under data protection law and how to use them
- What the Company is doing to comply with its legal obligations under data protection law.

Misuse of personal data, through loss, disclosure, or failure to comply with the data protection principles and rights of data subjects, may result in significant legal, financial and reputational damage.

In order to manage these risks, this policy sets out responsibilities for all managers, employees, contractors and anyone else who can access or use personal data in their work for the Company.

WHY THIS POLICY EXISTS

This data protection policy ensures that Pond Group Ltd

- Complies with data protection legislation and follows good practice;
- Protects the rights of staff, clients and partners;
- Is transparent about how it stores and processes individuals' data;
- Protects itself from risks of a data breach.

DATA PROTECTION LEGISLATION

Applicable data protection law including the EU General Data Protection Regulation (in force from 25 May 2018) describes how organisations, including Pond Group Ltd, must collect, handle and store personal information.

The rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with legislation, personal information must be obtained and used fairly, stored securely and not disclosed unlawfully.

Article 5 of the EU General Data Protection Regulation (GDPR) requires that personal data should be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

This policy sets out a framework of governance and accountability for data protection compliance across Pond Group Ltd. It forms part of the Company's Information Security Management System (ISMS). This incorporates all policies and procedures that are required to protect Company information by maintaining

- Confidentiality: protecting information from unauthorised access and disclosure

- Integrity: safeguarding the accuracy and completeness of information and preventing its unauthorised amendment or deletion
- Availability: ensuring that information is available only to authorised users whenever and wherever required
- Resilience: the ability to restore the availability and access to information, processing systems and services in a timely manner in the event of a physical or technical incident.

OBJECTIVES

PROCESS PERSONAL DATA FAIRLY AND LAWFULLY

This means that we will

- Only collect and use personal data in accordance with the lawful conditions set down under GDPR;
- Document each condition we rely on; maintain this information; review and update these records and make them available to the The Federal Commissioner for Data Protection and Freedom of Information (BfDI), other supervisory authorities and data subjects on request;
- Treat people fairly by using their personal data for the purposes and in a way that they would reasonably expect;
- Ensure that if we collect someone's personal data for one purpose, we will not reuse their data for a different purpose that the individual did not agree to or expect.

INFORM DATA SUBJECTS WHAT WE ARE DOING WITH THEIR PERSONAL DATA

At the point that we collect their personal data, we will explain to data subjects

- The identity and contact details of Pond Group Ltd and the Data Protection Officer;
- What personal data we collect;
- For what purposes we collect and use their data;
- What lawful conditions we rely on to process data for each purpose;
- Our obligations to protect their personal data;
- To whom we may disclose their data and why;
- How long we intend to retain their data;
- How to exercise their rights under data protection law.

UPHOLD INDIVIDUAL'S RIGHTS AS DATA SUBJECTS

Pond Group Ltd will uphold their rights to:

- Obtain a copy of the information comprising their personal data, free of charge within one month of receipt of their request; there are circumstances when a 'reasonable fee' may be charged if the request is manifestly unfounded or excessive, particularly if it is repetitive);
- Have inaccurate personal data rectified and incomplete data completed;
- Have their personal data erased when it is non longer needed, if the data has been unlawfully processed or if the data subject withdraws their consent, unless there is an overriding legal or public interest in continuing to process the data;

- Restrict the processing of their personal data until a dispute about the data's accuracy or use has been resolved, or when the Company no longer needs to keep personal data but the data subject needs the data for a legal claim.

APPLY 'DATA PROTECTION BY DESIGN AND DEFAULT' PRINCIPLES TO OUR PERSONAL DATA PROCESSING

Pond Group Ltd will

- Use proportionate privacy and information risk assessment and, where appropriate, data protection impact assessment, to identify and mitigate privacy risks at each stage of activity involving processing personal data and in managing upgrades or enhancements to systems and processes used to process personal data;
- Adopt data minimisation – we will collect, disclose and retain the minimum personal data for the minimum time necessary for the purpose;
- Anonymise personal data wherever necessary and appropriate, e.g. when using it for statistical purposes so that individuals can no longer be identified.

PROTECT PERSONAL DATA

Pond Group Ltd will use appropriate technical and organisational measures to

- Control access to personal data so that staff, contractors and other people working on the Company's business can only see such personal data as is necessary for them to fulfil their duties;
- Set and monitor compliance with security standards for the management of personal data as part of the Company's wider framework of information security policies and procedures;
- Reduce risks of exposure by pseudonymising personal data where possible;
- Provide appropriate tools for staff to use and communicate personal data securely when working remotely, such as through provision of a secure Virtual Private Network, encryption and firewall accounts;
- Manage all subject access requests for personal information about data subjects in accordance with procedures for responding to requests for personal data;
- Make appropriate and timely arrangements to ensure the confidential destruction of personal data in all media formats when it is no longer required for Company business.

MANAGE ANY BREACHES OF DATA SECURITY PROMPTLY AND APPROPRIATELY

Pond Group Ltd will take all necessary steps to reduce the impact of incidents involving personal data by following the Company's Information Security Incident Management Policy and Procedures.

When a data breach is likely to result in a risk to the rights and freedoms of data subjects, the Data Protection Officer will liaise with The Federal Commissioner for Data Protection and Freedom of Information (BfDI) and report the breach, in line with regulatory requirements, within 72 hours of discovery.

PEOPLE, RISKS AND RESPONSIBILITIES

POLICY SCOPE

This policy applies to

- Pond Group Ltd;
- All employees, staff and trainees of Pond Group Ltd;
- All contractors, suppliers and other people working on behalf of Pond Group Ltd.

It applies to all data that the Company holds relating to identifiable individuals, even if that information technically falls outside of the EU General Data Protection Regulation (GDPR).

RESPONSIBILITIES

All staff working at Pond Group Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

In addition, the following have key areas of responsibility:

- The Board of Directors is ultimately responsible for ensuring that Pond Group Ltd meets its legal obligations.
- The Data Protection Officer, Greg Gillies 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.
    - Arranging data protection training and advice for people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with data subject access requests.
    - Checking and approving any contracts or agreements with third parties that may handle the Company's sensitive data.

DATA STORAGE

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

- When not required, the paper or files should be kept in locked storage drawers and / or cabinets.

- Staff should ensure that paper and printouts are not left where unauthorised personnel can see them.

- Data printouts should be 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:

- Data should be protected by strong passwords that are changed regularly;
- Where data is stored in removable media, these should be kept locked away securely when not being used;
- Data should only be stored on Company designated drives and servers;
- Servers containing personal data is sited in a secure location, away from the general office space;
- Data is backed up frequently and backups tested regularly in line with the Company's standard backup procedures.
- All servers and computers containing data are protected by approved security software and a firewall.