

Company Procedures

Data Protection Policy

COMPANY PROCEDURE NO: CP4030

ISSUE NO 1

DATE: May 2018

Approved By:	
Julie Andrew	HR Director

Authorised for Issue By:	
Jenny Jones	Quality Assurance Manager



Data Protection Policy

Introduction

At APPH Limited (Heroux Devtek), we collect and process information about individuals (i.e. 'personal data') for business purposes, including employment and HR administration, provision of our services and business administration. This includes personal data relating to our employees, customers, suppliers and other third parties.

Compliance with data protection law is essential to ensure that personal data remains safe, our business operations are secure and the rights of individuals are respected. APPH Limited (Heroux Devtek) is a controller under data protection law, meaning it decides how and why it uses personal data. This Policy explains our procedures for complying with data protection law in relation to personal data. It also sets out your obligations whenever you are processing any personal data in the course of your employment.

If you routinely handle individuals' personal data, you will be given specific training/instructions regarding data protection procedures in relation to your particular role/department. These instructions will supplement your obligations as set out in this Policy.

There will also be other policies which will impact on how you deal with personal data and data protection. The main ones are our Information Security Policy and Cyber Security Policy and we expect you to comply with these where relevant.

This Policy does not give contractual rights to any Employees. It may be updated at any time.

Who does this Policy apply to?

This Policy applies to all APPH Limited (Heroux Devtek) employees, workers, contractors, agency workers, consultants, interns, volunteers, partners and directors, (together referred to as 'Employees' or 'you').

Who is responsible for data protection at APPH Limited (Heroux Devtek)?

The Board is ultimately responsible for APPH Limited (Heroux Devtek)'s compliance with applicable data protection law. APPH Limited (Heroux Devtek) has appointed a Data Compliance Manager who is responsible for overseeing and advising APPH Limited (Heroux Devtek) on and administering compliance with this Policy and data protection law. Other departmental managers have responsibilities under this policy such as IT Manager, Finance Director, Supply Chain Director. These responsibilities extend to implementing, monitoring and ensuring that all members of their teams adhere to this policy.

All Employees at APPH Limited (Heroux Devtek) have some responsibility for ensuring that personal data is kept secure and processed in a lawful manner although certain Employees will have particular responsibilities, of which they will be aware and in respect of which they may receive specific instructions.

If you are in any doubt about how you should handle personal data, or if you have any concerns or questions in relation to the operation (or suspected breaches) of this Policy, you should seek advice from the Data Compliance Manager (Human Resources Director) on ext 30501 (01928 530501) or in their absence another member of the Data Protection Team named above. Tel 01928 530530 or email GDPR@herouxdevtek.com

What is personal data?

Personal data means any information relating to any living individual (also known as a 'data subject') who can be identified (directly or indirectly) in particular by reference to an identifier (e.g. name, NI number, employee number, email address, physical features). Relevant individuals can include your colleagues, consumers, members of the public, business contacts, etc. Personal data can be factual (e.g. contact details or date of birth), an opinion about a person's actions or behaviour, or information that may otherwise impact on that individual. It can be personal or business related.

Personal data may be automated (e.g. electronic records such as computer files or in emails) or in manual records which are part of a filing system or are intended to form part of a filing system (e.g. structured paper files and archives).

What does 'processing' personal data mean?

'Processing' personal data means any activity that involves the use of personal data (e.g. obtaining, recording or holding the data, amending, retrieving, using, disclosing, sharing, erasing or destroying). It also includes sending or transferring personal data to third parties.

1. Processing personal data in a fair, lawful and transparent manner

Legal grounds for processing

Data protection law allows us to process personal data only where there are fair and legal grounds which justify using the information.

Examples of legal grounds for processing personal data include the following:

- complying with a legal obligation (e.g. health and safety or tax laws);
- entering into or performing a contract with the individual (e.g. an Employee's terms and conditions of employment, or a contract for services with an individual customer);
- acting in APPH Limited (Heroux Devtek) or a third party's legitimate interests (e.g. maintaining records of business activities, monitoring business productivity); and

Where consent is relied upon, it must be freely given, specific, informed and unambiguous, and APPH Limited (Heroux Devtek) must effectively demonstrate that consent has been given.



In line with ICO (Information Commissioner's Office) guidance regarding the employer/Employee relationship, APPH Limited (Heroux Devtek) does **not** use consent as a legal ground for processing Employee data unless the data processing activities concerned are genuinely optional.

In most cases, consent is also not required for other standard business activities involving use of customer or supplier data, but it may be needed for activities which are not required to manage the main business relationship.

Transparency

Data protection law also requires us to process personal data in a transparent manner by providing individuals with appropriate, clear and concise information about how we process their personal data.

We usually provide individuals with basic information about how we use their data on forms which collect data (such as application forms or website forms), and in longer privacy notices setting out details including: the types of personal data that we hold about them, how we use it, our legal grounds for processing the information, who we might share it with and how long we keep it for. For example, we provide information about our processing of Employees' personal data in APPH Limited (Heroux Devtek) Employee Privacy Notice.

We supplement these notices, where appropriate, with reminders or additional information at the time particular processing activities take place or become relevant for an individual (for example when they sign up for a new service or event).

2. Taking extra care when handling sensitive or special categories of personal data

Some categories of personal data are 'special' because they are particularly sensitive. These include information that reveals details of an individual's:

- physical or mental health, and;
- criminal offences or convictions.

Where special category personal data is concerned, data protection law requires us to have (as well as one of the legal grounds described in section 1), an additional legal ground to justify using this sensitive information. The appropriate legal ground will depend on the circumstances.

Additional legal grounds for processing special category data include the following. Those marked with an asterisk (*) would be particularly relevant to processing Employees' special category personal data:

- complying with a legal obligation/exercising a legal right in the field of employment*;
- assessing working capacity (based on expert medical opinion, and subject to obligations of confidentiality)*;
- exercising, establishing or defending legal claims*;



- preventing or detecting unlawful acts; or
- explicit consent of the individual. (As well as the requirements for consent outlined in section 1 above, this requires an express statement from the individual that their special category of data may be used for the intended purposes.)

3. Only processing personal data for specified, explicit and legitimate purposes

APPH Limited (Heroux Devtek) will only process personal data in accordance with our legitimate purposes to carry out our business operations and to administer employment and other business relationships.

4. Making sure that personal data is adequate, relevant and limited to what is necessary for your legitimate purposes

Data protection law requires us to ensure that, when we process personal data, it is adequate, relevant to our purposes and limited to what is necessary for those purposes (also known as 'data minimisation'). In other words, we ask for the information we need for our legitimate business purposes, but we won't ask for more information than we need in order to carry out our business operations.

5. Keeping personal data accurate and (where necessary) up-to-date

APPH Limited (Heroux Devtek) must take steps to ensure that personal data is accurate and (where necessary) kept up-to-date. For example, we request that Employees provide us with any change in contact details or personal information via form which can be obtained from the Human Resources department. We also take care that decisions impacting individuals are based on accurate and up-to-date information.

6. Keeping personal data for no longer than is necessary for the identified purposes

Records containing personal data should only be kept for as long as they are needed for the identified purposes. APPH Limited (Heroux Devtek) has in place data retention, storage and deletion policies and internal processes/guidelines regarding various types of company records and information that contain personal data.

We take appropriate steps to retain personal data only for so long as is necessary, taking into account the following criteria:

- the amount, nature, and sensitivity of the personal data;
- the risk of harm from unauthorised use or disclosure;
- the purposes for which we process the personal data and how long we need the particular data to achieve these purposes;
- how long the personal data is likely to remain accurate and up-to-date;
- for how long the personal data might be relevant to possible future legal claims; and



- any applicable legal, accounting, reporting or regulatory requirements that specify how long certain records must be kept.

Please see Employee Privacy Notice for the details of the retention periods.

7. Taking appropriate steps to keep personal data secure

Keeping personal data safe and complying with APPH Limited (Heroux Devtek) security procedures to protect the confidentiality, integrity, availability and resilience of personal data is a key responsibility for APPH Limited (Heroux Devtek) and its workforce.

APPH Limited (Heroux Devtek) also has a Cyber Security Policy setting out protocols for Employees on use of technology and communications systems, which also help to ensure appropriate security of personal data stored or communicated using such systems.

We regularly evaluate and test the effectiveness of these measures to ensure the security of our personal data processing activities.

8. Taking extra care when sharing or disclosing personal data

The sharing or disclosure of personal data is a type of processing, and therefore all the principles described in this Policy need to be applied.

Internal data sharing

APPH Limited (Heroux Devtek) ensures that personal data is only shared internally on a 'need to know' basis.

External data sharing

We will only share personal data with other third parties (including group entities) where we have a legitimate purpose, and an appropriate legal ground under data protection law which permits us to do so. Commonly, this could include situations where we are legally obliged to provide the information (e.g. to HMRC for tax purposes) or where necessary to perform our contractual duties to individuals (e.g. provision of information to our occupational pension providers).

We may appoint third party service providers (known as processors) who will handle information on our behalf, for example to provide payroll, data storage or other technology services.

APPH Limited (Heroux Devtek) remains responsible for ensuring that its processors comply with data protection law and this Policy in their handling of personal data. We must assess and apply data protection and information security measures prior to and during the appointment of a processor. The extent of these measures will vary depending on the nature of the activities, but will include appropriate risk assessments and reviews, and contractual obligations.

Routine disclosures of personal data to established recipients (e.g. payroll providers or group entities) which form a normal and regular part of your role and job duties will ordinarily



satisfy the above requirements. You should always ensure you comply with any particular APPH Limited (Heroux Devtek) instructions you are given. However, if you are in any doubt as to whether you can share personal data with anyone else, first contact the Data Compliance Manager (See “Who is Responsible for Data Protection pg 1)

9. Not transferring personal data to another country unless there are appropriate safeguards in place

An overseas transfer of personal data takes place when the data is transmitted or sent to, viewed, accessed or otherwise processed in, a different country. European Union data protection law restricts, in particular, personal data transfers to countries outside of the European Economic Area to ensure that the level of data protection afforded to individuals is not compromised (as the laws of such countries may not provide the same level of protection for personal data as within the EEA).

To ensure that data protection is not compromised when personal data is transferred to another country, APPH Limited (Heroux Devtek) assesses the risks of any transfer of personal data outside of the UK (taking into account the principles in this Policy, as well as the restrictions on transfers outside the EEA) and puts in place additional appropriate safeguards where required. For example, we currently: transfer person data to our Corporate Head Quarters in Canada. (Canada provides sufficient protection, rights and freedoms via PIPEDA law (Personal Information Protection & Electronic Documents Act) without the need for further protections)).

10. Reporting any data protection breaches without delay

APPH Limited (Heroux Devtek) takes any data protection breaches very seriously. These can include lost or mislaid equipment or data, use of inaccurate or excessive data, failure to address an individual's rights, accidental sending of data to the wrong person, unauthorised access to, use of or disclosure of data, deliberate attacks on APPH Limited (Heroux Devtek) systems or theft of records, and any equivalent breaches by APPH Limited (Heroux Devtek) service providers.

Where there has been a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to individuals' personal data, APPH Limited (Heroux Devtek) will take immediate steps to identify, assess and address it, including containing the risks, remedying the breach, and notifying appropriate parties (see below). APPH Limited (Heroux Devtek) has a **Breach Management Procedure** which sets out its procedures for identifying, assessing and addressing security breaches].

If APPH Limited (Heroux Devtek) discovers that there has been a personal data security breach that poses a risk to the rights and freedoms of individuals, we will report it to the ICO (Information Commissioner's Office) within 72 hours of discovery.

We also keep an internal record of all personal data breaches regardless of their effect and whether or not we report them to the ICO.



If a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures we have taken.

11. Not using profiling or automated decision-making unless you are authorised to do so

Profiling, or automated decision-making, occurs where an individual's personal data is processed and evaluated by automated means resulting in an important decision being taken in relation to that individual. This poses particular risks for individuals where a decision is based solely on that profiling or other automated processing.

One example of solely automated decision-making would be using an online psychometric test to automatically reject job applicants who do not meet a minimum pass mark (without any human oversight such as a review of the test results by a recruiting manager).

Data protection law prohibits decision-making based solely on profiling or other automated processing, except in very limited circumstances. In addition, where profiling or other automated decision-making *is* permitted, safeguards must be put in place and we must give individuals the opportunity to express their point of view and challenge the decision. We do not generally conduct profiling or other automated decision-making in respect of employees' or an individual's personal data.

12. Integrating data protection into operations

Data protection law requires APPH Limited (Heroux Devtek) to build data protection considerations and security measures into all of our operations that involve the processing of personal data, particularly at the start of a new project or activity which may impact on the privacy of individuals. This involves taking into account various factors including:

- the risks (and their likelihood and severity) posed by the processing for the rights and freedoms of individuals;
- technological capabilities;
- the cost of implementation; and
- the nature, scope, context and purposes of the processing of personal data.

We also seek to assess data protection risks regularly throughout the lifecycle of any project or activity which involves the use of personal data.

Individual Rights and Requests

Under data protection law, individuals have certain rights when it comes to how we handle their personal data. For example, an individual has the following rights:

- **The right to make a 'subject access request'**. This entitles an individual to receive a copy of the personal data we hold about them, together with information about how and why we process it and other rights which they have (as outlined below). This



enables them, for example, to check we are lawfully processing their data and to correct any inaccuracies.

- **The right to request that we correct incomplete or inaccurate** personal data that we hold about them.
- **The right to withdraw any consent** which they have given.
- **The right to request that we delete or remove** personal data that we hold about them where there is no good reason for us continuing to process it. Individuals also have the right to ask us to delete or remove their personal data where they have exercised their right to object to processing (Subject to the confines of the Data Retention Policy).
- **The right to object to our processing** of their personal data for direct marketing purposes, or where we are relying on our legitimate interest (or those of a third party), where we cannot show a compelling reason to continue the processing.
- **The right to request that we restrict our processing** of their personal data. This enables individuals to ask us to suspend the processing of personal data about them, for example if they want us to establish its accuracy or the reason for processing it.
- **The right to request that we transfer** to them or another party, in a structured format, their personal data which they have provided to us (also known as the right to 'data portability'). The applicability of this right depends on the legal grounds on which we process it.

We are required to comply with these rights without undue delay and, in respect of certain rights, within a one month timeframe.

Individuals also have rights to complain to the ICO about, and to take action in court to enforce their rights and seek compensation for damage suffered from, any breaches.

Record Keeping

In order to comply, and demonstrate our compliance, with data protection law, APPH Limited (Heroux Devtek) keeps various records of our data processing activities. These include a Record of Processing which must contain, as a minimum: the purposes of processing; categories of data subjects and personal data; categories of recipients of disclosures of data; information about international data transfers; envisaged retention periods; general descriptions of security measures applied; and certain additional details for special category data.

Training

We require all Employees to undergo some basic training to enable them to comply with data protection law and this policy. Additional training may be required for specific roles and activities involving the use of personal data.

To this end, we provide training as part of our induction process for new joiners to APPH Limited (Heroux Devtek) and operate an ongoing training programme to make sure that Employees' knowledge and understanding of what is necessary for compliance in the context of their role is up-to-date. Attendance at such training is mandatory and will be recorded.



Issue : 1
Date : May 2018
Page : 10 of 10

Departures from this Policy

There are some very limited exemptions from data protection law, which may permit departure from aspects of this Policy in certain circumstances.

You will be given specific instructions if any exemptions are relevant to your role.

If you think you should be able to depart from this Policy in any circumstances, you must contact the Data Compliance Manager/Data Compliance Team before taking any action.