IP Group Plc
Data Protection Policy

KEY POINTS

- IP Group will collect, store and process personal data about its workforce, portfolio companies, investors, website visitors and other people interacting with the company. The Company aims to protect all such information, ensuring its confidentiality, integrity and availability.

- The Data Protection Compliance Manager is responsible for ensuring compliance with the Data Protection Act 2018 ("**DPA**"), the retained EU law version of the General Data Protection Regulation as defined in the DPA ("**UK GDPR**") and this policy.

- IP Group will comply with the following ten data protection principles when processing any personal data.

POLICY

1. Introduction

IP Group has a responsibility to look after the information that we collect about individuals, including our business associates, employees and people browsing our websites. When people trust us with their information, we should live up to that trust.

Data protection laws give individuals the right to understand – and in some cases control – how their personal data is used. It also places obligations on IP Group to handle people's data fairly and to respect their rights.

IP Group takes its obligations under data protection laws seriously. A breach of our data protection responsibilities could result in a significant financial penalty, as well as negative publicity, damage to the Group's brands and perhaps most importantly, we could lose the trust of our business associates.

To protect against these risks, this Data Protection Policy and any accompanying guidelines should be read and followed by all IP Group staff. Any staff who fail to comply with this Policy and its accompanying guidelines may be subject to disciplinary action, up to and including dismissal.

If you have any questions about this Policy, you should contact your IP Group's Data Protection Compliance Manager, Will Crompton (will.crompton@ipgroupplc.com).

We are also subject to certain rules and privacy laws when engaging in direct marketing to our customers and prospective customers (for example, when sending marketing emails or making telephone sales calls). For more details on our approach to direct marketing please contact the Data Protection Compliance Manager.

2. Who and What is covered by this Policy?

This Policy applies to all IP Group businesses including operations, support functions and all staff (including permanent and temporary employees) and any third party personnel such as

agents, contractors and consultants, who have access to Personal Data processed by IP Group.

What is "Personal Data"? This Policy only applies to "***Personal Data***". That means information which relates to an identified or identifiable living individual (also known as 'a natural person'). It includes by way of example: names, addresses, email addresses, job applications, photographs, employment records, purchase histories, bank details and correspondence to and from an individual. Where it can be linked to an individual, it also includes web browsing information (e.g. cookie data) and IP addresses.

What about other confidential information? This Policy does not apply to confidential commercial information which is not Personal Data, e.g. financial information relating to a business.

What is "Sensitive Personal Data"? Certain Personal Data is designated as "***sensitive***" and given enhanced legal protections. Sensitive Personal Data is Personal Data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; biometric or genetic information; or information about a person's physical or mental health, sex life or sexual orientation. It is known in the law as 'special category personal data'.

What's "processing"? This Policy also talks about "***processing***" Personal Data. Processing essentially means *doing anything with* Personal Data; this includes collecting it, storing it, accessing it, combining it with other data, sharing it with a third party, and even deleting it.

IP Group processes Personal Data about our portfolio companies and prospective portfolio companies, our investors and prospective investors, our own staff, job applicants, staff at third party companies with whom we engage, our suppliers, candidates as part of our executive search function and people who attend our premises and browse our websites. All of this Personal Data should be treated in accordance with this Policy and special care should be taken in respect of Sensitive Personal Data.

3. IP Group' Data Protection Principles

IP Group's Data Protection Policy consists of the following Data Protection Principles (which include the principles set out in the UK GDPR relating to the Processing of Personal Data). Everyone at IP Group should follow our Data Protection Principles when processing Personal Data.

1. Fairness and Transparency: Give people information about how IP Group processes their Personal Data.

What does this mean?

We should be transparent and give people information about how we use their Personal Data. This also means not doing anything with their Personal Data which they would not expect or that we would be embarrassed for them to know about.

In particular, we should always tell people if their Personal Data will be passed to a third party. Similarly, if we receive Personal Data about an individual from a third party, we should make sure the individual knows about it as soon as we can.

This information is contained in our Privacy Policy, Fair Processing Policy and Candidate Privacy Notice (as applicable). If you are collecting Personal Data from an individual, directly or indirectly, then you must provide the individual with a Privacy Notice.

2. Lawful Processing: Make sure we always have a good, lawful reason to process Personal Data.

What does this mean?

This means that we need to make sure that we are legally allowed to process Personal Data.

IP Group should only process Personal Data if it can satisfy at least one of a number of conditions set out in data protection law (referred to as the lawful bases for processing). For IP Group, the most relevant of these are the following:

(i) The processing is necessary for the Company (or a third party's) legitimate interests, which are not overridden by any risk or harm to the rights or freedoms of the individuals. For example, the Company will need to process certain Personal Data relating to its employees in order to manage their performance, development and benefits etc.;

(ii) The processing is necessary for a contract with the individual. For example, we may need to process an employee's contact and bank details to provide them with their remuneration.

(iii) The processing is necessary to comply with a legal obligation;

(iv) The processing is necessary for IP Group (or a third party's) legitimate interests, which are not overridden by any risk or harm to the individuals. For example, IP Group will need to process certain Personal Data relating to its employees in order to manage their performance, development and benefits etc; or.

(v) The individual has consented. Note that the UK GDPR sets a high standard for consent. Before relying on consent as a lawful basis for processing, we should consider if consent is required or if any other lawful bases are more appropriate.

We must identify and document the legal basis being relied upon for each processing activity. If consent is required or if you need more information on the lawful bases for processing, please contact the Data Protection Compliance Manager.

Where we rely on consent, individuals must be easily able to withdraw their consent at any time and withdrawal must be promptly honoured. Consents may also need to be refreshed if the purposes for processing have changed.

IP Group should only process Sensitive Personal Data in exceptional circumstances. As well as a lawful basis, you will need to satisfy additional conditions to be able to process this type of data. Therefore, please consult the Data Protection Compliance Manager before doing so.

3. Purpose Limitation: Only collect Personal Data for a specific business need of IP Group. If we want to reuse the Personal Data for a new purpose, we must make sure the two are compatible.

What does this mean?

We should always have a clear purpose for any Personal Data before we collect it, and this should reflect a specific business need of IP Group.

If IP Group later wants to use the Personal Data for a new or different purpose or share it with a new third party, we should consider whether it is compatible with the original purpose, and whether it would be within the reasonable expectations of the individual to whom the Personal Data relates. If you want to use Personal Data for a new or different purpose from that for which it was obtained, you should first contact the Data Protection Compliance Manager for advice on how to do this in compliance with both the law and this Data Protection Policy.

Before starting any new processing or collecting any new data, you should speak to the Data Protection Compliance Manager to ensure data protection and privacy is considered from the outset. If there could be risks associated with any new processing, together with the Data Protection Compliance Manager, you should conduct a Data Protection Impact Assessment ("**DPIA**") to decide whether any safeguards need to be put in place to protect the individuals. The Data Protection Compliance Manager shall have primary responsibility for completing the DPIA, however the relevant employee shall be required to provide all necessary information and assistance to the Data Protection Compliance Manager to enable the DPIA to be completed. For more information on conducting DPIAs, please refer to the *DPIA Guidelines*.

4. Data Minimisation: Only process as much Personal Data as we need, and no more.

What does this mean?

In any particular case, IP Group should only collect or otherwise process as much Personal Data as it needs for that specific purpose. This means we should not collect Personal Data that we do not need, or ask for Personal Data 'just in case' it may be useful.

Before asking for or accessing information about someone, you should ask yourself whether you *really* need that information to achieve your result.

5. Accuracy: Keep Personal Data accurate, complete and up-to-date.

What does this mean?

Wherever possible, IP Group should give individuals the opportunity to amend or correct their Personal Data (and offer a self-service tool where possible, for example, our Bamboo HR system). If we independently become aware of Personal Data which is inaccurate or out-of-date, we should take reasonable steps to correct it or delete it.

All members of staff should inform HR about any changes in their Personal Data processed by IP Group where self-service is not available.

6. Retention: Only keep Personal Data for as long as we need it. If we don't need the Personal Data anymore, we must delete it or anonymise it.

What does this mean?

IP Group should only keep Personal Data for as long as it is required for its specified purpose. Once the Personal Data is no longer needed, it should be deleted, or anonymised so that individuals can no longer be identified from it. This applies to all Personal Data processed by IP Group, including any Personal Data that members of staff may store locally for business purposes. Please refer to our data retention information in the *Employee Fair Processing Notice* and the *Data Archiving Guidelines* for further information.

7. Security: Protect IP Group's Personal Data from getting lost or stolen. Make sure our service providers protect our Personal Data as well.

What does this mean?

We must make sure we always protect Personal Data with appropriate security measures, to prevent any accidental or unauthorised access, damage, loss or disclosure.

If you become aware of any actual or suspected loss or breach of security relating to Personal Data, you should immediately report it to your Manager, the Head of Operations and IT and the Data Protection Compliance Manager, in line with our *IT Policy*.

This Security Principle extends to our service providers who handle Personal Data on our behalf. IP Group should only appoint service providers who can provide appropriate protection for our Personal Data. You should consult the Data Protection Compliance Manager before appointing any service provider who will have access to IP Group's Personal Data, even where the provider is offering a free or inexpensive service or trial (for example this could be a provider of a new IT system).

8. Individual Rights: Allow individuals the right to access, correct or erase their Personal Data, or object to it being used for certain purposes.

What does this mean?

Anyone whose Personal Data we process has the right to obtain a copy of that Personal Data, and to correct any inaccuracies. This applies to employees as well as any other person whose Personal Data we hold. In certain circumstances, they also have a right to have their Personal Data erased or not used for a particular purpose. Likewise, where we rely on consent as a lawful basis for processing, individuals who have given their consent have the right to withdraw their consent at any time. IP Group must respect these rights, and respond to requests in accordance with our legal obligations. IP Group is also entitled to refuse requests in certain circumstances.

If you receive a request from an individual relating to their Personal Data, you should consult the Data Protection Compliance Manager immediately. It is your responsibility to report any request from an individual relating to their Personal Data to the Data Protection Compliance Manager. A copy of IP Group's *Response Procedures for Data Subject Requests* can be provided by the Data Protection Compliance Manager.

9. Personal Data Transfers: Put in place safeguards before sending Personal Data outside the UK.

What does this mean?

Generally, we should not share Personal Data with third parties unless certain safeguards and UK GDPR compliant contractual arrangements have been put in place.

Likewise, because data protection standards may not be the same in countries outside the United Kingdom ("**UK**"), UK data protection laws place restrictions on when Personal Data may be transferred outside the UK. The transfer will only be allowed if certain safeguards are put in place to protect the Personal Data, wherever it goes. Even though we are headquartered in the UK (and when our servers are located there), we may have staff, suppliers and other group companies based elsewhere, and therefore we need to be mindful that these types of restrictions exist.

These restrictions apply whether IP Group is sending Personal Data to a third party (e.g. a US-based cloud provider) or another company within our group. Importantly, the restrictions apply not only when the Personal Data will be stored in the non-UK country, but also if the Personal Data will only be accessed remotely from that country (e.g. if a third party IT service provider or one of our staff members based outside the UK has remote access to Personal Data on our systems in the UK).

You should consult the Data Protection Compliance Manager before sending Personal Data outside the UK or allowing a party outside the UK to have access to our Personal Data stored within the UK.

10. Accountability: IP Group will take steps to make sure our processing of Personal Data complies with this Policy.

What does this mean?

IP Group is responsible for ensuring our processing of Personal Data is compliant with the law. That is why we have implemented this Data Protection Policy, as well as any accompanying guidelines.

IP Group will conduct training for all staff who handle Personal Data on their responsibilities under this Policy. It is the responsibility of everyone working at IP Group to comply with this Policy and complete their required training.

This Policy will be periodically reviewed and updated as necessary to ensure that they are effective and meet IP Group's requirements.

This Policy was last updated in November 2023.