Data Protection Policy

Introduction

The BDP Group acknowledges that everyone has rights with regard to the way in which their personal data is handled. BDP collects, stores and processes personal data about our employees and the employees of other members of BDP Group, clients, suppliers and other third parties. BDP recognises that the correct and lawful treatment of this data will maintain confidence in the organisation and provide for successful business operations.

About this Policy

This policy applies to all individuals working within, and for, the BDP Group at all levels and grades, including directors, senior managers, staff, consultants, contractors, seconded staff, agency staff, agents or any other person associated with us or any of our subsidiaries or their employees, wherever located.

This policy, and the other documents referred to in it, sets out what we expect from you in order for BDP to comply with applicable law and you must read, understand and comply with this policy when processing personal data on our behalf. Compliance with this policy is mandatory and any breach may result in disciplinary action.

This policy, and any other documents referred to in it, also sets out the basis on which BDP will process any personal data it collects from data subjects, or that is provided to BDP by data subjects or other sources. It also sets out rules on data protection and the legal conditions that must be satisfied when BDP obtains, handles, processes, transfers and stores personal data.

The types of personal data that BDP may be required to handle include information about current, past and prospective employees of BDP and other members of the BDP Group, suppliers, contractors and clients (and their respective employees) and others that BDP communicates with. It may also include data gathered as the result of project requirements, such as the personal data of respondents to surveys undertaken as part of public consultations. The personal data, which may be held on paper, electronically or in any other media, is subject to certain legal safeguards specified in various data protection legislation.

In preparing this policy, we have carefully considered the legal and regulatory requirements which apply to the BDP Group, these include the EU General Data Protection Regulation (GDPR), the UK GDPR and other national laws and rules within the various jurisdictions in which we operate around the world. For the purposes of the EU GDPR and UK GDPR, BDP is a controller of personal data (which means we are responsible for deciding how and why personal data are used).

Our Principles

Any processing of personal data must comply with the data protection principles we adhere to which are set out in the legislation relevant to the country where the data is being gathered and / or processed. These are that personal data must be:

- Processed fairly and lawfully and in a transparent manner.

- Obtained only for one or more specified, explicit and legitimate purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Not be kept in a form which permits identification of data subjects for longer than is necessary for the purpose or purposes for which it is processed.
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Not transferred to or accessed from other countries or territories unless legally permitted and after implementing appropriate contractual, technical and organisational measures to safeguard the personal data.

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above. Data subjects have a number of rights in relation to the data we hold about them (including rights to access their data) which we must respect.

BDP Data Protection Team

BDP has a Data Protection Team which can provide advice and assistance to BDP Group staff in relation to the processing of personal data, and you should contact us with any questions you have regarding the processing of personal data.

There are some circumstances where staff **must** contact the BDP Data Protection Team, for example:

- In the event of a security breach (contact us immediately)
- If a request is received from a data subject regarding their personal data (contact us immediately)
- Before processing, if you are unsure whether or not processing is permitted
- Before sharing or disclosing personal data with third parties
- Before transferring data internationally (unless this is expressly permitted by BDP's existing policies)
- Before processing sensitive or special category data (such as medical information) or other high-risk data (such as financial information)
- Before engaging in any new or high-risk processing activities which might pose a risk to individuals or their data protection rights. In these cases, a data protection impact assessment (DPIA) or other risk assessment will be required).

As stated above, you must contact the BDP Data Protection Team, using the email address, BDPDataProtection@bdp.com immediately if you suspect there has been a personal data breach or receive a request from an individual regarding their personal data, sometimes referred to as a Subject Access Request (SAR).

You should also refer to the BDP Data Protection Team if you have any concerns that the policy has not been followed or if you have any questions about the operation of this policy, such as:

- you are unsure about the retention period for the personal data being processed
- you are unsure about what security or other measures BDP has in place to protect personal data
- you are unsure on what basis you can transfer personal data
- you have been asked by a client to provide personal data other than a CV or photograph as part of a bid or submission

Fair and Lawful Processing

Data protection laws are not intended to prevent the processing of personal data, but to ensure that it is done lawfully, fairly and in a transparent manner and without adversely affecting the rights of the data subject.

For example, under EU GDPR and UK GDPR, in order for personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the legislation which can include, among other things, (i) the data subject's express and freely given consent to the processing, (ii) the processing is necessary for the performance of a contract with the data subject, (iii) the processing is necessary for the compliance with a legal obligation to which the data controller is subject (e.g. health and safety or employment laws), or (iv) for the legitimate interest of the data controller or the party to whom the data is disclosed, provided that this interest is not overridden by the interests of the data subject.

When sensitive personal data (some of which is also known as 'special category' data) is being processed, additional conditions must be met (and data relating to criminal convictions must not be processed except in very limited circumstances). When processing personal data as data controllers in the course of BDP's business, BDP will ensure that those requirements are met.

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
- Contact the BDP Data Protection Team for assistance in difficult situations. No-one should be bullied into disclosing personal information.

Consent

Much of the personal data processing carried out by BDP is regulated by the EU GDPR and / or the UK GDPR, both of which require us to have a 'legal basis' for processing. Consent is one of the lawful bases that we can use to process personal data. However, there are a

number of conditions that have to be satisfied for consent to be effective and these are generally difficult to satisfy in relation to employees. Accordingly, unless consent is specifically required by applicable law, it is our policy to avoid relying on consent as a basis for processing of data where another lawful basis (e.g. legitimate interests or compliance with a legal obligation) may be available.

From time to time, we may ask for your consent to process certain information about you which you can refuse.. If you do provide your consent to processing, you can subsequently withdraw your consent to us doing so at any time by sending a request to the contact details at the end of this notice.

Where consent is sought in relation to the processing of personal data you must obtain guidance from the BDP Data Protection Team in advance by emailing **BDPDataProtection@bdp.com**.

Processing for Limited Purposes

Data protection laws, including the EU GDPR and UK GDPR require that data is processed fairly and in a transparent manner. BDP will comply with its legal obligations, which typically include only processing personal data for the specific, explicit and legitimate purposes notified to the data subject when the data was first collected. As required by law, BDP will notify those purposes to the data subject when the data is first collected or at any point where personal data is processed for a purpose other than that for which the personal data was originally collected.

BDP will hold and process personal data about its employees in manual and automated filing systems as set out in the Employee Privacy Notice.

Where any services or benefits provided to BDP or the BDP Group by third parties, for example for pension administration or health insurance / benefits, BDP may disclose employees' personal information to those third parties, but will take reasonable steps to ensure that such data is held securely.

Sensitive Data

Some personal data, such as financial, medical, equality, diversity and inclusion (EDI) information and other highly personal data is especially sensitive and must be handled with special care. In some cases, additional legal requirements will apply, such as under the EU GDPR and UK GDPR which impose additional legal obligations when processing ‘Special Category Data’ or ‘sensitive’ personal data such as health data, data relating to ethnic origin, religious beliefs, trade union membership, political affiliation, or data relating to the commission of an offence.

BDP may process sensitive personal data about its employees where necessary in connection with its rights and duties as an employer, for example health data in relation to absences and workforce management / administration, insurance or benefits, EDI monitoring data and other sensitive information. Further information about BDP’s approach to this type of data can be found in BDP’s Special Category Data Policy. If you intend to process

sensitive personal data, or any other personal data which could reasonably be considered as especially risky, before doing so you must consult the BDP Data Protection Team.

Notifying Data Subjects

Where BDP collects personal data directly from data subjects, we will inform them about:

- The purpose or purposes for which BDP intends to process that personal data.
- The types of third parties, if any, with which BDP will share or to which BDP will disclose that personal data.
- The means, if any, by which data subjects can limit BDP's use and disclosure of their personal data.

Adequate, Relevant and Non-Excessive Processing

BDP will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

Accurate Data

BDP will endeavour to ensure that personal data it holds is accurate and kept up to date. BDP will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Employees are responsible for ensuring that they keep the following information up to date using YourData as relevant; name, address, personal email address, emergency contact details, bank account information and any applicable EDI information.

BDP will take reasonable steps to destroy or amend inaccurate or out-of-date data where the employee is unable to amend their personal records independently.

Timely Processing

BDP will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. BDP will take all reasonable steps to destroy, or erase from its systems, all data which is no longer required.

For more information on our data retention periods please contact us on the details at the end of this notice.

Data Subject Rights

Data subjects may make a formal request , sometimes referred to as a Subject Access Request (SAR), for information that BDP holds about them. Any such request can be made in writing or verbally. Any such request must follow BDP's SAR procedure and be sent immediately to the BDP Data Protection Team. BDP will comply with its legal obligations in respect of any request it receives.

BDP will process all personal data in line with data subjects' rights under applicable law. In some cases this may include disclosing, correcting, restricting or erasing personal data in response to a data subject, for example the EU GDPR and UK GDPR permit individuals the following specific rights in relation to their personal data:

- The right of access – this enables individuals to receive further information about the personal data we hold about them as well as to obtain a copy of that data
- The right to rectification – this enables individuals to have any incomplete or inaccurate personal data that we hold about them corrected
- The right to erasure (also known as the 'right to be forgotten') – in limited circumstances an individual can ask us to delete personal data we hold about them, for example where it is no longer required for the purposes for which it was collected/processed
- The right to restrict processing – in limited circumstances an individual can ask us to suspend the processing of their personal data
- The right to data portability – in limited circumstances an individual can ask us to transfer their personal data to another organisation
- The right to object – this enables an individual to object to us processing their personal information in limited circumstances

It is important to remember that these rights are not universal nor are they absolute. The data subject rights available to an individual (and the extent to which they can be exercised) will depend on the circumstances, including the BDP Group company processing the personal data and the data protection laws to which it is subject. There are also a number of circumstances where BDP may be entitled to refuse to comply with a request. However, in any event, BDP will usually be required to respond within a short deadline and, therefore, it is essential that any request from a data subject is notified to BDP's Data Protection Team immediately by emailing **BDPDataProtection@bdp.com**.

Data Security

BDP has implemented appropriate technical and organisational security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

BDP will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if they have confirmed they comply with the requirements of applicable data protection legislation.

BDP will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed

- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on BDP's central computer system with appropriate filing security and not on individual PC hard drives.

Security procedures include:

- **Entry controls**. Any stranger seen in entry-controlled areas should be reported to the appropriate Office Manager.
- **Secure lockable desks and cupboards**. Desks and cupboards should be kept locked if they hold confidential information of any kind. Personal information is always considered confidential.
- **Methods of disposal**. Paper documents should be shredded or disposed of in the studio confidential waste bins provided. Digital storage devices should be cleared down in a secure manner or physically destroyed when they are no longer required.
- **Equipment**. Data users must ensure that individual monitors do not show confidential information to passers-by and that they lock their PC when it is left unattended.

You must not make electronic recordings (whether on your own or the Company's devices) of any external or internal meetings or conversations, unless all parties agree and the recording is authorised by your line manager or Director. Any unauthorised electronic recordings create risks in respect of, for example, confidential information and / or our data protection obligations to our employees and third parties. Unauthorised recordings will be treated as a disciplinary matter which could result in your employment being terminated.

As set out in the BDP Use and Misuse of IT, Communications and Systems Policy, BDP will monitor user activity on the Internet at network level for the purposes of security and integrity of the BDP network. This extends to PCs, laptops and personal devices connected to the BDP network both wirelessly and through wired connections. Monitoring also continues of BDP devices when used remotely, with user activity automatically reviewed when devices are next connected to the network. This includes user identification (SSID and IP address), domain names of websites visited, duration of visits, and all files downloaded from the Internet. Staff should be aware that this monitoring may reveal sensitive data about them, for example visits to websites which detail the activities of a particular political party or religious group might indicate the political opinion or religious belief of that individual. Staff should maintain their own personal privacy by not using BDP's systems to access this type of information. Staff should also acknowledge that all internet activity logs are regularly backed up with records maintained as necessary for the stability and robustness of BDP's overall IT systems.

It is important to note that BDP policies, including this one, apply to all BDP supplied devices (including desktops, laptops, smartphones and tablets) whether used inside or away from the office and any personal devices connected to any BDP network.

Transferring Personal Data

BDP may transfer personal data to (or allow access to it from), but not limited to, BDP Group's personnel based in the UK, Dublin, Rotterdam, China, India, Canada, Singapore, USA and Middle East.

BDP and the BDP Group will take the required steps to ensure that an adequate level of protection is in place in relation to the transfer and processing of such personal data. We have in place agreements between our Group companies to ensure your personal data is treated by all of our Group companies in a way that is consistent with various data protection laws. However, you should not permit personal data to be transferred outside your jurisdiction without first consulting the BDP Data Protection Team. For these purposes a transfer includes sending data overseas (including by email), making data available to access or view overseas, or using international systems (such as cloud and web-based systems).

Disclosure and Sharing of Personal Information

BDP may share personal data we hold with any member of our Group, which means any subsidiaries or holding companies of Building Design Partnership Limited and Nippon Koei Co., Ltd. We will only share personal data as is necessary and permitted by law, and will do so in accordance with this policy.

BDP may also disclose personal data it holds to third parties:

- With our brokers, agents, insurers and / or professional advisors for the placing of benefits and insurances.
- With other companies within the current, and future Group for project collaboration and intercompany transfers.
- With other third party contractors who provide services to us such as pension providers, in relation to insurance benefits and suppliers of our IT systems when required to enable them to provide services to us. Further information is available from local HR.
- With clients and potential clients where it is required to enable us to provide a service to them and to respond to tenders.
- In the event that BDP sells or buys any business or assets, in which case it may disclose personal data it holds to the prospective seller or buyer of such business or assets.
- To third parties where required to protect BDP's rights, property, or the safety of BDP employees, clients or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.
- To police, government and other regulatory authorities where we are required to do so or we are requested to do so and we consider it is appropriate to do so in the circumstances.

We will disclose personal data to third parties who provide services to BDP (for example, suppliers and contractors). Where this occurs, it is important to ensure that there is a written contract in place which includes provisions governing the use, disclosure and deletion of the personal data. In some cases, such as where EU GDPR or UK GDPR applies, there are specific legal requirements which a contract with a processor (being a person such as a supplier who uses personal data on our behalf) must meet. Accordingly, before sharing or disclosing personal data with third parties you must always consult the BDP Data Protection Team.

Review and Monitoring of this Policy

This policy, which is non-contractual, will be monitored at a minimum annually by the BDP GDPR Compliance group to ensure it is up to date and achieving its objectives and may be amended from time to time.

Responsibility for the Policy

For the purposes of this policy, the BDP Data Protection Team will have primary responsibility for the regular review and update where appropriate. The responsibility for the appropriate and effective application of the policy across each studio is with the Studio Chair (UK) or Studio Leader (International).

This is BDP's Data Protection Policy and as Chief Executive I commit myself and the Company to it.

Nick Fairham
Chief Executive

Date: 1 July 2024

Definition of Data Protection Terms

Data is any information which is stored electronically (e.g. on a computer, mobile phone, tablet or other device), or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom BDP hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information. In BDP, data subjects include current, past and prospective employees, and employees of (and individual contacts at) suppliers, contractors and clients.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in BDP's possession or which BDP is likely to be able to access). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions or behaviour.

Controller(s) are the people who, or organisations which, determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the GDPR. BDP is the controller of all personal data used in its business for its own purposes.

Data users are those of BDP's employees whose work involves handling ('processing' in Data Protection terms - see below) personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times. Data users are likely to include people in 'Administration' roles (including: HR and the HR Network, Central employees, HR, business and financial software users) Project Management and Directors

Processors include any person or organisation that is not a data user that processes personal data on BDP's behalf and on BDP's instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on BDP's behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

GDPR means the General Data Protection Regulation which is effective from 25 May 2018.

Sensitive Personal Data (also known as **Special Category Data**) includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, genetic or biometric make-up, or sexual life or orientation. For the purpose of this policy It also includes information about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and in some cases may condition require the express permission of the person concerned. This information is detailed in the Special Category Data Policy.