

BDP Privacy Policy

Introduction

Welcome to BDP's privacy policy in relation to collecting personal data through the Commonplace online consultation tool.

BDP respects your privacy and is committed to protecting your personal data. This privacy policy will inform you as to how we look after your personal data when you visit our website (regardless of where you visit it from) and tell you about your privacy rights and how the law protects you.

This Privacy Policy was last updated on 8th July 2022.

Building Design Partnership Limited is a company registered in England under number 2207415.

1. Important information and who we are

1.1 Purpose of this privacy policy

This privacy policy aims to give you information on how BDP collects and processes your personal data that we collect from you, or that you provide to us.

It is important that you read this privacy policy together with any other privacy policy or fair processing policy we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This privacy policy supplements other notices and privacy policies and is not intended to override them.

Controller

Victoria Business Improvement District is the Controller and responsible for your personal data.

Processor

Building Design Partnership Limited is the Processor and responsible for processing your personal data (collectively referred to as "BDP", "we", "us" or "our" in this privacy policy).

The BDP GDPR Compliance group is responsible for overseeing questions in relation to this privacy policy. If you have any questions about this privacy policy, including any requests to exercise your legal rights, please contact the BDP GDPR Compliance group using the details set out below.

1.2 Contact details

Our full details are:

Full name of legal entity: Building Design Partnership Limited

Name or title of Data Protection Manager: GDPR Compliance Group

Email address: BDPDataProtection@bdp.com

Postal address: 11 Ducie Street, Piccadilly Basin, PO Box 85, Manchester M60 3JA

Telephone number: 0161 828 2200

1.3 You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK regulator for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

1.4 It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

2. The data we collect about you

2.1 Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

2.2 The personal data we collect includes but is not limited to: name, email address, postal address, telephone number, the company you work for, job title and the industry you work in.

2.3 We also collect data relating to your race, ethnicity and health which is classed as 'Special Category' personal data.

2.3.1 This particular data will however be anonymised upon collection and therefore cannot be linked to or identify you.

2.3.2 The collection of Special Category data is necessary in this instance to ensure we are collecting a diverse range of responses to our consultation. We are following Westminster City Council's guidance on early community engagement which states that: *"It is important to engage with as many members of communities affected by proposals, from as diverse a cross section of those communities, as possible."*

3. How is your personal data collected?

3.1 Your data will be collected through the information you provide on the Commonplace website.

4. How we use your personal data

4.1 We will only use your personal data for the purposes for which we collected it, in this instance:

4.1.1 To register and provide you access to the Commonplace website so that you can participate in the consultation.

4.1.2 To provide you with updates on the project as it progresses.

4.1.3 To maintain our own records as proof of the consultation process.

5. Who your data will be shared with

5.1 Your data will be shared with relevant project partners (architects and landscape designers for example) so that the feedback you provide can be incorporated into the scheme. We require all third

parties to respect the security of your personal data, to treat it in accordance with the law and only process it in accordance with our instructions.

- 5.2 The Commonplace website collects some personal data about you for its own purposes which falls outside the scope of the contract we have with them. More information on this can be found in Commonplace's Privacy Policy [here](#).

6. If you wish to remain publicly anonymous

- 6.1 If you contribute to a Commonplace, your feedback and any agreements added by you, are anonymised before being made available publicly to anyone who has an interest in the information. The words of your feedback and your agreements may be used for further analysis or to provide examples of feedback in marketing material, but your identity will not be revealed unless you shared something in your comment that reveals your identity.
- 6.2 If you do not want to be identified with material posted by you then you should not include your name or any identifying information in the material posted, whether you post the material as a typed comment or a recorded voice comment. We do not review feedback before it's published, so it is important that you take responsibility for this yourself.

7. Our lawful basis for processing

- 7.1 We will only use your personal data when the law allows us to. In this instance we are relying on our Legitimate Interests under Article 6(1)(f) of the UK GDPR.
- 7.2 In relation to Special Category data, we are relying on your consent under Article 9 (2)(a) UK GDPR. You have the right to withdraw this consent at any time by contacting us.

8. Data security and storage

- 8.1 We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. The storage is encrypted and access controlled.
- 8.2 In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.
- 8.3 We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

9. Data retention

- 9.1 Your personal data will be retained for the duration of the project for which you have provided feedback and comment.
- 9.1.1 In some circumstances you can ask us to delete your data: see 'Request erasure' below for further information.

- 9.1.2 In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

10. Your legal rights

- 10.1 Under certain circumstances, you have rights under data protection laws in relation to your personal data.
- 10.1.1 **Request access** to your personal data (commonly known as a ‘**data subject access request**’). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- 10.1.1 **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- 10.1.2 **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- 10.1.3 **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
- 10.1.4 **Request restriction of processing** of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- 10.1.5 **Request the transfer of** your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- 10.1.6 **Withdraw consent** at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

If you wish to exercise any of the rights set out above, please contact us at BDPDataProtection@bdp.com or in writing at the office address at the beginning of this policy document.

10.2 No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

10.3 What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

10.4 Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

11. Complaints

11.1 You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

12. Glossary

12.1 **Legitimate Interest** means those pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

12.2 **Special Category** means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.