

BIG YELLOW SELF STORAGE COMPANY LIMITED (“BIG YELLOW”)

WORKFORCE DATA PRIVACY NOTICE

1. ABOUT THIS DATA PRIVACY NOTICE

- 1.1 This notice is designed to provide information on how Big Yellow (referred to as “we”, “us” or “our”) processes the personal data of its workforce (referred to as “you” or “your”) in accordance with the General Data Protection Regulation and, when enacted, the Data Protection Act 2018 (together referred to as the “GDPR”). This notice applies to current and former members of our workforce, including employees, workers, agency workers, and self-employed consultants.
- 1.2 As a “data controller”, we are responsible for deciding how we process personal data about you. We take your privacy seriously and we are fully committed to protecting your personal data at all times. We will only process your personal data in accordance with applicable data protection laws, adhering to the principles (as applicable) contained in the GDPR.
- 1.3 This notice does not form part of your contract of employment and we may amend it at any time to reflect any changes in the way in which we process your personal data. We will provide you with a new privacy notice when we make any substantial updates, and we may also notify you in other ways from time to time about the processing of your personal data.

2. THE KIND OF INFORMATION WE HOLD ABOUT YOU

- 2.1 “Personal data” is any information about a living individual from which they can be identified such as name, ID number, location data, any online identifier, or any factor specific to the physical, physiological, genetic, mental, economic or social identity of that person. It does not include data where any potential identifiers have been removed (anonymous data) or data held in an unstructured file.
- 2.2 There are “special categories” of more sensitive personal data which are more private in nature and therefore require a higher level of protection, such as genetic data, biometric data, sexual orientation, race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and health.
- 2.3 When we refer to “processing”, this means anything from collecting, using, storing, transferring, disclosing, altering or destroying personal data.

3. RECEIVING YOUR PERSONAL DATA

- 3.1 We may obtain personal data and / or special category personal data about you from third party sources, such as recruitment agencies, job boards, previous employers or

referees, LinkedIn, occupational health professionals, HMRC, the Department for Work and Pensions, brokers and pension providers. Where we receive such information from these third parties, we will only use it in accordance with this notice and in line with our Data Protection Policies¹. In some cases, they will be acting as a controller of your personal data and therefore we advise you to read their privacy notice and / or data protection policy.

4. HOW WE USE YOUR PERSONAL DATA

4.1 We process your personal data for various reasons, relying on a variety of different bases for lawful processing under data protection law, as set out below.

4.1.1 **To comply with our legal obligations.** This may include:

- eligibility to work in the UK checks as required by immigration laws, such as passport and visa documentation;
- payroll records, social security, child maintenance, marital status, student loans and national insurance information, to comply with social security and HMRC (tax) requirements;
- information in relation to legal claims made by you or against you, in order to comply with court processes and court orders;
- information relating to the occurrence, investigation or prevention of fraud, such as through a whistleblowing complaint; and
- pension benefits to comply with pension legislation.

4.1.2 **To prepare for and to perform the contract of employment you have entered in to with us.** This may include:

- formal identification documentation relating to you, such as a passport or full birth certificate and national insurance document to verify your identity (including your date of birth);
- your contact details such as your name, address, telephone number and personal email address which will be used to communicate with you on employment matters during your employment;
- bank details which are used to send / receive funds to / from you such as payment of your salary, salary reviews/advances, bonus, expenses, statutory sick pay, company sick pay, statutory maternity / paternity / adoption / shared parental leave pay, or to make or repay loans or advances of salary;

¹ Our Data Protection Policies can be found at the following link <https://tinyurl.com/ybbegeej> in the Information Governance & Security section of our intranet.

- incentive plans and save as you earn scheme relating to you in order to comply with the terms of any such scheme;
- information relating to the enrolment or renewal of your employment benefits including pension, private health care, childcare vouchers, cycle to work scheme, life assurance and permanent health insurance in order to provide you with these benefits (where applicable); and
- details of the terms and conditions of your employment.

4.1.3 **To pursue our (or a third party's) legitimate interests as a business.** This may include:

- training records, appraisals and 1:1 meeting notes about you in order to assist / assess your career development and training needs and / or to ensure that you are properly managed and supervised;
- information relating to the performance of your employment duties, such as disciplinary records, as this is relevant to your ability to carry out your job and for us to assess and identify areas in which we may need to help you improve;
- information relating to the performance of your duties may also be used to conduct an investigation if circumstances warrant it and to take appropriate action either for conduct or capability reasons in accordance with our Problem Solving and Disciplinary Procedures;
- information relating to any grievance process involving you, in order that an investigation may be conducted and appropriate action taken (if any) in accordance with our Problem Solving and Disciplinary Procedures;
- management reports (including statistical and audit information) to ensure workplace efficiencies are maximised;
- health, safety and environmental information (including records and information relating to your next of kin) to ensure that we are complying with relevant policies and procedures. This also allows us to implement any training where applicable;
- work related contact details on our intranet and / or internal systems to facilitate efficient communication within the business;
- voicemails, emails, correspondence and other work-related communications created, stored or transmitted by you using our computer or communications equipment for the purposes of the efficient management of the business in accordance with our IT Policies;

- non-medical absence records and details including holiday records, appointments, jury service, maternity, paternity, adoption and parental leave in order to monitor attendance levels and to comply with our policies;
- capturing photographs / images for internal and external normal business purposes (i.e. email accounts, intranet, external marketing, HR platform etc.) in order to assist employee engagement and harmonisation of the business;
- CCTV (operated within all of the Company's stores and car parks) to ensure business efficiencies, for staff and customer security reasons, for the protection of our property, crime prevention and for health and safety reasons, in accordance with our CCTV Policy; and
- network and information security data in order for us to take steps to protect your information against loss, theft or unauthorised access.

4.1.4 **Where you have consented to specific processing.** This may include:

- information disclosed to a third party agency relating to your pay details for the purposes of providing tenancy references;
- information disclosed to a mortgage provider relating to your employment history and pay details for the purposes of a mortgage application; and
- information disclosed to a prospective future employer relating to your employment details for the purposes of providing a reference.

4.1.5 **Where it is in your vital interests.** This may include information about allergies or any medical conditions so as to prevent any unnecessary accidents, and advise medical professionals in the event of an emergency.

4.2 Where you have consented to specific processing of your personal or special categories data, you have the unequivocal right to withdraw your consent at any time by indicating your withdrawal in a written format to a member of the Human Resources team.

4.3 Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data.

4.4 We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

5. HOW WE USE YOUR SPECIAL CATEGORY PERSONAL DATA

5.1 We also collect, store and use your special category personal data for a range of reasons, relying on a variety of different bases for lawful processing under the GDPR.

5.1.1 **To enable us to perform our legal obligations in respect of employment, social security, and social protection law**, in line with our Data Protection Policies. This may include:

- information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws;
- information gathered as part of a whistleblowing investigation;
- information relating to you involving allegations of unlawful discrimination, in order that an investigation may be conducted and appropriate action taken (if any) under our Problem Solving and Disciplinary Procedures; and
- health information to assess and / or to comply with our obligations under employment, equal opportunities and health and safety legislation (for example a requirement to make reasonable adjustments to your working conditions).

5.1.2 **For occupational health reasons or where we are assessing your working capability**, subject to appropriate confidentiality safeguards. This may include:

- information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits;
- sickness absence records, such as statement of fitness to work, reasons for absence and self-certification forms; and
- records of return to work interviews / meetings.

5.1.3 **Where it is needed for statistical purposes in the public interest**, such as for equal opportunities monitoring, in line with our Data Protection Policies. To ensure meaningful equal opportunities monitoring and reporting, we will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, and your sexual life or orientation.

5.1.4 **To establish, defend or exercise legal claims in an employment tribunal or any other court of law.**

5.1.5 **Where you have given explicit consent to the processing of special categories of data, such as** capturing photographs / images for exceptional business purposes (i.e. external media activities).

6 INFORMATION ABOUT CRIMINAL CONVICTIONS

- 6.1 We envisage that we will hold information about criminal convictions.
- 6.2 We will only collect this information if it is appropriate given the nature of your role and where the law allows us to do so. This will usually be where such processing is **necessary for reasons of substantial public interest**, provided that we do so in line with our Data Protection Policies. We may collect this information as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.
- 6.3 We will use information about criminal offences and convictions in the following ways:
- To prevent or detect unlawful acts;
 - To protect the public against dishonesty; and / or
 - To prevent fraud.
- 6.4 Where we process criminal convictions information about you, whether as part of any application process or otherwise, we will retain criminal conviction information for the duration of your employment.

7 AUTOMATED DECISION MAKING / PROFILING

- 7.1 We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

8 DATA SHARING

- 8.1 We may share your personal data and special category personal data internally. In particular, it may be shared with: Human Resources employees involved in the recruitment process, employee relations and / or in the administration of your employment; line managers; consultants; advisers; or other appropriate persons who we shall make you aware of from time to time.
- 8.2 We may share your personal data and special category personal data with other companies within our Group, this includes Big Yellow Group PLC and its associated companies including Big Yellow Self Storage Company Limited, Armadillo Self Storage Limited and Armadillo Self Storage 2 Limited. They may use your personal data as part of our regular reporting activities on performance, in the context of a business reorganisation or group restructuring exercise, health and safety and suspected fraudulent activity. They may also use your personal data if you have submitted an application for a job vacancy within the wider group.
- 8.3 We may share your personal data and special category personal data with third parties, agents, subcontractors and other organisations (as listed below) where it is

necessary to administer the working relationship with you or where we have a legitimate interest in doing so:

- occupational health providers;
- payroll providers (including but not limited to Cascade);
- financial product / services providers (including auditors);
- training providers;
- recruitment and employment agencies;
- insurance brokers (including but not limited to Brent's and Pure Protection)
- employee benefits providers (including but not limited to Sodexo (childcare voucher platform), Metlife (life assurance provider), Aviva (permanent health insurance), AXA (pension provider) and YBS (SAYE scheme provider));
- employee reward providers (including but not limited to Voucher Express, Red Letter Days, John Lewis, M&S, Debenhams, Moonpig and Funky Pigeon);
- insurance providers;
- providers of IT services; and
- providers of legal services.

8.4 When we disclose your personal data to third parties as listed above, we only disclose to them any personal data that is necessary for them to provide their service. We have contracts in place with these third parties in receipt of your personal data requiring them to keep your personal data secure and not to use it other than in accordance with our specific instructions.

8.5 We only disclose your personal data to third parties who we are sure have adequate policies / procedures in place in relation to data security.

8.6 We may also share your personal data and special category personal data with other third parties for other reasons. For example, in the context of the possible sale or restructuring of the business; to provide information to a regulator; or to otherwise comply with the law. To comply with our legal obligations we may share your data with the following, all of whom are obliged to have adequate policies / procedures in place in relation to data security:

- HMRC for tax purposes;
- Home Office for immigration purposes; and
- student loan agencies to ensure that appropriate reductions are made from your salary.

- 8.7 We may share your personal data with third parties such as mortgage providers, property rental providers or prospective future employers (as stated at 4.1.4) with your consent.

9 TRANSFERRING INFORMATION OUTSIDE THE EEA

- 9.1 We do not envisage that we will transfer your personal data outside of the EEA (meaning the EU 27 member states including Norway, Iceland and Liechtenstein), however we will notify you in writing if this position changes.

10 DATA STORAGE AND SECURITY

- 10.1 Your personal data and special category personal data is stored in a variety of locations, including: electronically on our secure servers / in hard copy form in access-restricted rooms or locked filing cabinets.
- 10.2 More information as to where specific categories of personal data are stored can be found out by asking a member of the Human Resources team.
- 10.3 We take appropriate technical and organisational security measures and have rules and procedures in place to guard against unauthorised access, improper use, alteration, disclosure and destruction and accidental loss of your personal data. Information about the IT security standards that we use to protect your personal data is contained in our Information Security Policy.
- 10.4 In addition, we limit access (by setting levels of permission) to your personal information to those members of our workforce who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.
- 10.5 We have put in place procedures to deal with any suspected or actual data security breach and will notify you and the Information Commissioner's Office ("ICO") of a suspected breach where we are legally required to do so.
- 10.6 Whenever we propose using new technologies, or where processing is construed as 'high risk', we are obliged to carry out a Data Protection Impact Assessment which allows us to make sure appropriate security measures are always in place in relation to the processing of your personal data.

11 DATA RETENTION

- 11.1 We keep your personal data and special category personal data for as long as is necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements, but typically we keep your

personal data and special category personal data for the duration of your employment and then retain records of:-

- 11.1.1 Employee personnel files for 7 years after termination;
 - 11.1.2 Payroll information for 7 years after termination; and
 - 11.1.3 Health and safety information for 40 years after termination.
- 11.2 At the expiry of the set retention period, or in other select circumstances, your personal data will be permanently and securely deleted. Further details of our data retention periods and processes can be found in our Data Retention Policy.
- 11.3 In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use and retain such information without further notice to you, as it falls outside of the definition of personal data under the GDPR.

12 YOUR DUTIES

- 12.1 We encourage you to ensure that the personal data that we hold about you is accurate and up to date by keeping us informed of any changes to your personal data. You can update your details by notifying HR.
- 12.2 As a member of our workforce, you also have obligations under various data protection laws. Our policies on data protection are set out in our Data Protection Policies. You are required to be familiar with and comply with these rules and procedures.

13 YOUR RIGHTS

- 13.1 You may make a formal request for access to personal data and or special category data that we hold about you at any time. This is known as a Subject Access Request. We must respond to this request within a certain time period (being 40 days under the Data Protection Act 1998, reducing to one month under the GDPR from 25 May 2018). Please note that under the GDPR we are permitted to extend the one month time period for responding by an additional two months where in our view your request is complex or numerous in nature. We may also charge a reasonable fee based on administrative costs where in our view your request is manifestly unfounded, excessive or a request for further copies. Alternatively, we may refuse to comply with the request in such circumstances. For further details on subject access requests and the types of request listed below, please refer to our Data Protection Policies.
- 13.2 Under certain circumstances, by law you also have the right to request:
- 13.2.1 to have your personal data corrected where it is inaccurate;

- 13.2.2 to have your personal data erased where it is no longer required. Provided that we do not have any continuing lawful reason to continue processing your personal data, we will make reasonable efforts to comply with your request;
- 13.2.3 that your personal data be transferred to another person in an appropriate format;
- 13.2.4 withdraw your consent to processing where this is our lawful basis for doing so;
- 13.2.5 to restrict the processing of your personal data where you believe it is unlawful for us to do so, you have objected to its use and our investigation is pending, or you require us to keep it in connection with legal proceedings; and
- 13.2.6 to object to the processing of your personal data, where we rely on **legitimate business** interests as a lawful reason for the processing of your data. You also have the right to object where we are processing your personal information for direct marketing purposes. We have a duty to investigate the matter within a reasonable time and take action where it is deemed necessary. Except for the purposes for which we are sure we can continue to process your personal data, we will temporarily stop processing your personal data in line with your objection until we have investigated the matter. If we agree that your objection is justified in accordance with your rights, we will permanently stop using your data for those purposes. Otherwise, we will provide you with our justification as to why we need to continue using your data.
- 13.3 The way we process your personal data and the legal basis on which we rely to process it may affect the extent to which these rights apply. If you would like to exercise any of these rights, please address them in writing to the HR Department.
- 13.4 We may need to request specific information from you to help us to confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is an appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.
 - 13.4.1 In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Human Resources Department. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to. If you withdraw your consent, our use of your personal data before your withdrawal is still lawful.
 - 13.5 You may complain to a supervisory body if you are concerned about the way we have processed your personal data. In the UK this is the ICO – www.ico.org.uk. Although

you have the right to complain to the ICO, we encourage you to contact us first with a view to letting us help in resolving any queries or questions.

14 QUESTIONS

- 14.1 If you have any questions about any matter relating to data protection or the personal data and/or special category personal data that that we process about you, please contact the Human Resources Department.