

## Data Breach (Data Loss) Policy

### Introduction

Croudace Homes Group Limited, which for the purposes of this Policy includes all companies within the Croudace group (**Croudace Homes Group**) is committed to complying with data protection law and to respecting the privacy rights of individuals.

This Data Breach Policy ("**Policy**") sets out our approach to breaches of data protection law.

References in this Policy to "us", "we", "ourselves" and "our" are to Croudace Homes Group. References to "you", "yourself" and "your" are to all those to whom this Policy applies.

"Our data" refers to both data generated by us, and data of customers, prospective customers, employees or prospective employees, consultants, contractors and third parties.

It is your responsibility to familiarise yourself with this Policy and to apply and implement its requirements in the event of a data breach.

Data protection law, including the law as it relates to a data breach, is a complex area. This Policy has been designed to ensure that you are aware of the legal requirements imposed on you and on us in the event of a data breach and to give you practical guidance on how to comply with them. However, this Policy is not an exhaustive statement of our or your responsibilities in relation to a data breach. If at any time you have any queries on this Policy, your responsibilities or any aspect of data protection law, seek advice. Contact your line manager, Caroline Bailey, or Alison Clegg.

This Policy works in conjunction with other policies implemented by us from time to time, including for example the Data Protection Policy and the E-mail Internet and CCTV Policy along with any other policies we implement from time to time.

### **Who is responsible for action in the event of a Data Breach?**

We are not required to appoint a Data Protection Officer. However we have appointed

- Company Secretary and Group Legal Director Caroline Bailey to be responsible for overseeing our overall compliance with data protection laws and she has the title of Data Compliance Officer; and
- Principal Company Solicitor Alison Clegg to be responsible for the reporting of data breaches and in the event of a data breach she must be contacted immediately (see "**What you must do in the event of a breach**" below)

All our employees are responsible for data protection, and each person has their role to play to make sure that we are compliant with data protection laws.

### **Breach of this Policy**

Any breaches of this Policy will be viewed very seriously. All personnel must read this Policy carefully and make sure they are familiar with it. Breaching this Policy is a disciplinary offence and will be dealt with under our Disciplinary Policy.

If you do not comply with data protection laws and/or this Policy, then you are encouraged to report this fact immediately to our Data Compliance Officer. This self-reporting will be taken into account in assessing how to deal with any breach, including any non-compliances that may pre-date this Policy coming into force.

Also if you are aware of or believe that any other representative of ours is not complying with data protection laws and/or this Policy you should report it in confidence to our Data Compliance Officer. Our Whistleblowing Procedure will apply in these circumstances and you may choose to report any non-compliance or breach through our confidential whistleblowing reporting facility.

## **Data Protection Law**

The General Data Protection Regulation (**GDPR**) and the Data Protection Act 2018 (“**DPA 2018**”) (together “**data protection laws**”) are the main legislation in the UK covering Data Protection.

This Policy states the position as at March 2024.

## **How to recognise a data breach**

A data breach includes any loss of data owned or used by us, whether a third party obtains access to the data or not. As examples this will include (but is not limited to)

- Loss of a computer, laptop, mobile telephone or removable storage media
- Loss of our data stored on a computer or server due to corruption of the hard drive
- Loss of physical papers or files containing our data
- Hacking of our computer network and systems or a computer network and system that processes data for us
- A ransomware, malware, virus or other malicious code attack made to our computer network and systems
- Non secure destruction of our data
- Sending an email or post to the wrong person which contains our data or personal data of a customer employee or third party
- Sending an email to a group of recipients using the "to" field when their email addresses should not have been disclosed to the other recipients
- Allowing someone to overhear a telephone conversation when identifying details are disclosed
- Data being disclosed or revealed to someone else in the organisation who is not entitled to see or know that data

The above is not an exhaustive list, and data losses and breaches can take many forms. If anything involves loss of our data or unauthorised third party access to our data and that data relates to an individual in any way, then it will be a data breach under data protection laws. For the rest of this Policy we have used the term “data

loss” as this is less confusing. We also require reporting of data losses, whether or not the data relates to an individual, so any type of data loss should be reported to us.

Compliance with our Acceptable Use Policy, Bring Your Own Device Policy and Data Protection Policy and any other security policies and a common sense approach to keeping data safe are critical. You should always treat and keep data secure and safe as if it was your own personal information, and treat it with respect as you would want your own personal information to be treated.

### **What you must do in the event of a breach**

As soon as you become aware of any data loss which involves our data, or any data we process on behalf of anyone else, you must **IMMEDIATELY** notify Alison Clegg, Principal Company Solicitor by email to both [gdpr@croudace.co.uk](mailto:gdpr@croudace.co.uk) and [alison.clegg@croudace.co.uk](mailto:alison.clegg@croudace.co.uk) and by telephone 07557 032674. You must also make sure that you receive a delivery receipt for the e-mail. If you cannot speak to Alison Clegg then you must immediately contact one of the individuals below by ringing 01883 346464

Caroline Bailey

Simon Boakes

Marina Waller

Sonia Dad

You will need to supply details and background regarding the data loss or breach including details of the type of data lost, the amount of data lost, who it relates to, how it was lost, the identity of any third party who has acquired the data (if known). You must also provide any other information that may be requested by us, and in some cases we may need you to complete a form detailing the data loss with as much information as you have available.

Even if you do not have all of this information available straight away, then do not delay in making notification of the data loss to us. Time is critical.

The notification requirement applies whether or not you were involved in or the cause of the data loss. If you are aware of a data loss then you must notify it to us regardless of its cause.

We will treat all notifications which are about a colleague or another worker in confidence in accordance with our whistleblowing policy.

### **Failure to notify**

You must notify a data loss in accordance with this policy, even if you are at fault in causing or contributing to the data loss, for example due to human error, the fact that you have reported it will work in your favour. It is a fact of life that data losses sometimes occur, often due to human error or the need to improve our systems and procedures.

If you are aware of a data loss in relation to our data or data we process on behalf of a third party and you fail to notify that data loss in accordance with this Policy, then we will regard that as serious misconduct if you are an employee.

If you are a third party supplier to us, and you are aware of a data loss in relation to our data or data we process on behalf of a third party and you fail to notify that data loss in accordance with this Policy, then we will regard that as a material and serious breach of contract.

This applies whether the data loss was caused or contributed to by you or if you are just aware of a data loss caused or contributed to by a colleague or third party or even just aware of a data loss where no-one was at fault.

### **Why you must notify**

Under Data Protection laws we are under a duty to inform the regulator (in the UK this is the Information Commissioners Office or ICO) of data losses involving personal data which we control in cases where the data loss may result in harm to individuals.

We have to inform the ICO as soon as possible and in any event within 72 hours of becoming aware of the data loss. This time period runs from when you become aware

of the data loss, and not when you notify the data loss or breach in accordance with this Policy. Therefore the notification to us in accordance with this Policy must be made immediately.

Your notification will allow us to assess whether or not we need to notify the ICO regarding the data loss.

If we fail to notify the ICO when we should then we can be subject to fines of up to 2% of group worldwide turnover or £8.7 million, whichever is the higher. These are very substantial risks and for this reason the failure to notify us of any data loss which you are aware of is treated as serious misconduct, and could result in dismissal or termination of a contract.

Also if we are processing data on behalf of a third party, then that third party will require us to inform them of the data loss involving their data as soon as possible as they will be subject to the same risks. It is also a legal requirement under Data Protection laws that we do so this as soon as possible. If we do not, then as well as breaching the contract with the third party, we can also be liable for the same level of fines as if it were our data.

### **What happens once you have notified**

Once you have notified a data loss, we will assess what needs to happen next. It may be that we have to report the data loss to the ICO, in which case we may need you to fill in as much as possible of a form that we will send to you. This is to obtain the background information necessary to be able to report the data loss properly.

Make sure that you complete the form and provide the information as quickly as possible, as we will be under very short timescales to report the data loss to the ICO.

We may also need to report the data loss to the individuals whose data is affected by the data breach.

We may also need to take steps to try to mitigate the impact of the data loss, contain the data loss or reverse the data loss. These steps are easier to take if we know about the data loss as soon as possible and without any delays.

We may also need to change our systems, procedures and protections to prevent or reduce the risk of such a data loss occurring in the future. There is usually something to be learnt from a data loss.

Whatever happens we will record the data loss on our data loss register, which may help us to spot patterns or areas of particular risk over time so that we can take steps to prevent or reduce the risk of repeat data losses.

## **QUERIES AND UPDATES**

We may update this Policy from time to time, and you will be made aware of any material updates or changes to this Policy.

If you think that we could improve our data protection processes and protections, then let your Data Compliance Officer know by email at [gdpr@croudace.co.uk](mailto:gdpr@croudace.co.uk) with your suggestion.

Similarly, if you have any questions regarding this policy then please contact your Data Compliance Officer by email at [gdpr@croudace.co.uk](mailto:gdpr@croudace.co.uk).