croudacegroup

Data Protection 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 Protection Policy ("**Policy**") sets out our approach to data protection law and the principles that we will apply to our processing of personal data. The aim of this Policy is to ensure that we process personal data in accordance with the law and with the utmost care and respect.

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

We recognise that you have an important role to play in achieving the aim set out above. It is your responsibility, therefore, to familiarise yourself with this Policy and to apply and implement its requirements when processing any personal data.

Data protection law 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 and to give you practical guidance on how to comply with them. This Policy also sets out the consequences of failing to comply with these legal requirements. However, this Policy is not an exhaustive statement of data protection law nor of our or your responsibilities in relation to data protection. 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 or Caroline Bailey, the Data Compliance Officer (by e-mail: gdpr@croudace.co.uk).

Who is responsible for data protection?

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.

We are not required to appoint a Data Protection Officer or DPO as they are commonly referred to. However we have appointed the Company Secretary and Group Legal Director Caroline Bailey to be responsible for overseeing our compliance with data protection laws and she has the title of Data Compliance Officer.

Why do we have a data protection policy?

We recognise that processing of individuals' personal data in a careful and respectful manner cultivates trusting relationships with those individuals and trust in our brand. We believe that such relationships will enable our organisation to work more effectively with and to provide a better service to those individuals.

The overarching aim and message of this Policy is to treat personal data with care and respect. You should use or process or protect personal data only in a way that you would be happy with and expect if it was your own personal data being used or processed by a third party organisation. If this would not the case then it is likely that what you want to do with personal data is not permitted and you should seek advice from our Data Compliance Officer.

This Policy works in conjunction with other policies implemented by us from time to time, including for example the Data Breach Policy, the Data Retention Policy, the Whistle Blowing Policy, and the IT Policies along with any other policies we implement from time to time.

Breach

Status of this Policy and the implications of breach.

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 Procedure.

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 which 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. This includes any contractor or third party supplier that we may use or have a relationship with. Our Whistle Blowing procedure will apply in these circumstances and you may choose to report any non-compliance or breach through our confidential Whistle Blowing reporting facility (see our Whistle Blowing Policy).

Other consequences of breach

There are a number of serious consequences for both yourself and us if we do not comply with data protection laws. These include:

For you:

Disciplinary action: Your terms and conditions of employment require you to comply with our policies. Failure to do so could lead to disciplinary action including dismissal.

Criminal sanctions: Serious breaches could potentially result in criminal liability for you personally.

Investigations and interviews: Your actions could be investigated and you could be interviewed in relation to any non-compliance.

For the organisation:

Criminal sanctions: Non-compliance could involve a criminal offence.

Civil Fines: These can be up to £17.5 million or 4% of group worldwide turnover whichever is higher. These amounts are very substantial.

Assessments, investigations and enforcement action: We could be assessed or investigated by, and obliged to provide information to, the Information Commissioner on our processes and procedures and/or be subject to the Information Commissioner's powers of entry, inspection and seizure causing disruption and embarrassment.

Court orders: These may require us to implement measures or take steps in relation to, or cease or refrain from, processing personal data.

Claims for compensation: Individuals may make claims for damage they have suffered as a result of our non-compliance.

Bad publicity: Assessments, investigations and enforcement action by, and complaints to, the Information Commissioner quickly become public knowledge and might damage our brand. Court proceedings are public knowledge.

Loss of business: Prospective customers, customers, suppliers and contractors might not want to deal with us if we are viewed as careless with personal data or disregarding our legal obligations in relation to personal data.

Use of management time and resources: Dealing with assessments, investigations, enforcement action, complaints, claims, etc takes time and effort and can involve considerable cost.

Data Protection Law

The UK 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.

The data protection laws all require that the personal data is processed in accordance with the Data Protection Principles (on which see below) and gives individuals rights to access, correct and control how we use their personal data (on which see below).

Outline

The main themes of the data protection laws are:

- good practices for handling personal data;
- transparency for data subjects as to how personal data is used;
- rights for individuals in respect of personal data that controllers hold on them; and
- being able to demonstrate compliance with data protection laws.

Key words in relation to data protection

The following are key terms that are commonly used in relation to data protection:

Personal data is data that relates to a living individual who can be identified from that data (or from that data and other information in or likely to come into our possession). That living individual might be an employee, customer, prospective customer, supplier, contractor or contact, and that personal data might be written, oral or visual (e.g. CCTV). See below for further examples of "Personal Data".

Identifiable means that the individual can be distinguished from a group of individuals (although the name of that individual need not be ascertainable). The data might identify an individual on its own (e.g. if a name or video footage) or might do if taken together with other information available to or obtainable us (e.g. a job title and company name). More details on this can be found in part 2 of this Policy.

Data subject is the living individual to whom the relevant personal data relates.

Processing is widely defined under data protection law and generally any action taken by us in respect of personal data will fall under the definition, including for example collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure, storage or destruction of personal data, including CCTV images.

Controller is the person who decides how personal data is used, for example we will always be a controller in respect of personal data relating to our employees. You may also hear a controller being referred to as a data controller and they mean the same thing.

Processor is a person who processes personal data on behalf of a controller and only processes that personal data in accordance with instructions from the controller, for example an outsourced payroll provider will be a processor. You may also hear a processor being referred to as a data processor and they mean the same thing

Personal data

Data will relate to an individual and therefore be their personal data if it:

- identifies the individual. For instance, names, addresses, telephone numbers and email addresses;
- its content is about the individual personally. For instance, medical records, credit history, a recording of their actions, or contact details;
- relates to property of the individual, for example their home, their car or other possessions;
- it could be processed to learn, record or decide something about the individual (or this is a consequence of processing). For instance, if you are able to link the data to the individual to tell you something about them, this will relate to the individual (e.g. salary details for a post where there is only one named individual in that post, or a telephone bill for the occupier of a property where there is only one occupant);
- is biographical in a significant sense, that is it does more than record the individual's connection with or involvement in a matter or event which has no personal connotations for them. For instance, if an individual's name appears on a list of attendees of an organisation's meeting this may not relate to the individual and may be more likely to relate to the company they represent;
- has the individual as its focus, that is the information relates to the individual personally rather than to some other person or a transaction

or event they were involved in. For instance, if a work meeting is to discuss an individual's performance this is likely to relate to the individual;

- affects the individual's privacy, whether in their personal, family, organisation or professional capacity, for instance, email address or location and work email addresses can also be personal data;
- is an expression of opinion about the individual; or
- is an indication of our (or any other person's) intentions towards the individual (e.g. how a complaint by that individual will be dealt with).

Information about companies or other legal persons who are not living individuals is not personal data. However, information about directors, shareholders, officers and employees of a company is often personal data, so business information to companies can often be personal data. Information relating to sole traders or partnerships is always personal data as they are not separate legal entities from their business activities. Therefore it is best to work on the basis that all business related information is personal data, unless it clearly relates only to a corporate entity.

Examples of information likely to constitute personal data:

- Unique names;
- Names together with email addresses or other contact details;
- Job title and employer (especially if there is only one person in the position);
- Information about individuals obtained as a result of Anti Money Laundering checks or credit checks;
- Customer profile information (e.g. preferences); and
- Financial information and accounts (e.g. information about tax liabilities, income, expenditure, credit history)

In addition information relating to a plot is likely to be classed as personal data relating to a purchaser if it is created after exchange of contracts between Croudace and that purchaser or it just relates to the purchaser, e.g. details of any optional extras they may have selected for the plot they wish to purchase or the terms of their reservation

agreement. However information which relates a development as a whole or which was created prior to exchange of contracts and does not relate to a particular purchaser is unlikely to be personal data of a purchaser of an individual plot.

The main requirements

In summary, the data protection laws require a controller to:

- only process personal data for certain purposes;
- process personal data in accordance with the 6 principles of 'good information handling' (including keeping personal data secure, processing it fairly and in a transparent manner and keeping it for no longer than is required); see "Data Protection Principles" below;
- provide certain information to those individuals about whom we process personal data which is usually provided in a "privacy notice", for example you will receive one of these from us as one of our staff;
- respect the rights of those individuals about whom we process personal data (including providing them with access to the personal data we hold on them); and
- keep adequate records of how data is processed and, where necessary, notify the regulator and possibly data subjects where there has been a data breach.

Every member of our staff has an important role to play in complying with these requirements. It is your responsibility, therefore, to familiarise yourself with this Policy.

Data protection law in the UK is enforced by the Information Commissioner's Office ("**ICO**") and they are the regulator for data protection in the UK. The ICO has extensive powers, including the ability to impose civil fines of up to £17.5 million or 4% of group worldwide turnover, whichever is higher. Also the data protection laws can be enforced in the courts and the courts have the power to award compensation to individuals.

Data protection principles

The data protection laws set out 6 principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:

- processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;
- collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes (“purpose limitation”);
- adequate and relevant, and limited to what is necessary to the purposes for which it is processed (“data minimisation”);
- accurate and where necessary kept up to date;
- kept for no longer than is necessary for the purpose (“storage limitation”);
- processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures (“integrity and security”).

In addition a controller must be able to demonstrate accountability, which essentially means not only are data protection laws being complied with but also being able to demonstrate and evidence that compliance. That usually requires keeping various written records and having policies (such as this Policy) to be able to demonstrate compliance.

Processing Data

Lawful basis for processing personal data

For personal data to be processed lawfully, we must process it on one of the legal grounds set out in the data protection laws.

For the processing of ordinary personal data in our organisation these may include, among other things:

- the data subject has given their consent to the processing;
- the processing is necessary for the performance of a contract with the data subject;
- the processing is necessary to protect the vital interests of the data subject or another natural person;
- the processing is necessary for the compliance with a legal obligation to which we are subject; or

- the processing is necessary for the legitimate interest reasons of Croudace Homes Group or a third party.

Lawful basis for processing special category personal data

Special category personal data under the data protection laws is personal data relating to an individual's race, political opinions, health, religious or other beliefs, trade union records, sex life, biometric data and genetic data.

Under data protection laws this type of information is known as special category personal data and criminal records and history is its own special category which is treated for some parts the same as special category personal data. Previously these types of personal data were referred to as sensitive personal data and some people may continue to use this term.

To lawfully process special categories of personal data we must, as well as having one of the legal basis for processing ordinary personal data, also ensure that either the individual has given their explicit consent to the processing or that another of the following conditions has been met:

- the processing is necessary for the performance of our obligations or exercising specific rights under employment law and social security and social protection law;
- the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent. The Information Commissioner's Office ("ICO") has previously indicated that this condition is unlikely to be met other than in a life or death or other extreme situation;
- the processing relates to information manifestly made public by the data subject;
- the processing is necessary for the purpose of establishing exercising or defending legal claims; or
- the processing is necessary for the purpose of preventative or occupational medicine or for the assessment of the working capacity of an employee.

To lawfully process personal data relating to criminal records and history there are even more limited reasons, and we must either:

- ensure that either the individual has given their explicit consent to the processing; or
- ensure that our processing of those criminal records history is necessary under a legal requirement imposed upon us.

We would normally only expect to process special category personal data or criminal records and history data in a Human Resources context or in the context of our customers for Help to Buy Properties. However it can sometimes be relevant for other customers, for example if we make adjustments to a plot requested by the purchaser to better facilitate wheelchair access.

Whilst we are always obliged to protect and keep personal data safe and only allow access to it by our staff who need to see and use that personal data for the purposes of their work, there are even higher standards applied for special category personal data or criminal records and history data due to the sensitivity of such information.

When do we process personal data?

Virtually anything we do with personal data is processing including collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure, storing or destruction. So even just storage of personal data is a form of processing. We might process personal data using computers or manually by keeping paper records.

Examples of processing personal data might include:

- Using personal data to correspond with or contact customers;
- Holding personal data in our databases or documents and most of our records will contain at least some personal data; and
- Recording personal data in personnel or customer files.

Data subject rights

Under data protection laws individuals have certain rights (**Rights**) in relation to their own personal data. In summary these are:

- The rights to access their personal data, usually referred to as a subject access request
- The right to have their personal data rectified;
- The right to have their personal data erased, usually referred to as the right to be forgotten;
- The right to restrict processing of their personal data;
- The right to object to receiving direct marketing materials;
- The right to portability of their personal data;
- The right to object to processing of their personal data;
- The right to withdraw any previous given consent; and
- The right not to be subject to a decision made solely by automated data processing.

The exercise of these Rights may be made in writing, including email, and also verbally and should be responded to in writing by us and actioned by us (if we are the relevant controller) without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. We must inform the individual of any such extension within one month of receipt of the request, together with the reasons for the delay, but it is best to inform the individual data subject straight away.

Where we need further information from a data subject in order to be able to action their Rights request, for example we need some proof of their identity or the nature of their request needs to be clarified so we can comply with it, then this will be dealt with by our Data Compliance Officer. As long as we do genuinely need the further information then time will not run during the period that we are waiting for it from the data subject, but such requests for further information must not be used as delaying tactic by us.

Where the data subject makes the Rights request by electronic means, any information is to be provided by electronic means where possible, unless otherwise requested by the individual.

If we receive the Rights request from a third party (e.g. a legal advisor), we must take steps to verify that the Rights request was, in fact, instigated by the individual and that the third party is properly authorised to make the Rights request. This will usually mean contacting the relevant individual directly to verify that the third party is properly authorised to make the Rights request, unless it is obvious from the circumstances.

We also need to exercise particular care where the personal data of one data subject is linked with the personal data of another data subject. This is often the case with joint purchasers of a plot, where a Rights request by one of the joint purchasers for a data subject access request does not entitle them to see and be provided with the personal data of the other joint purchaser. In these cases it is often easiest to see if the other joint purchaser will join in with the Right's request and if they each confirm that they are happy with their personal data being provided to the other joint purchaser. Otherwise we may need to remove or redact personal data relating to the other joint purchaser. A similar position can arise where a Rights request relates to CCTV and the CCTV images cover more than one individual, though in those cases it is often not possible to obtain consent from the other individuals so if it is not possible to obscure the other individuals in those images we may need to weigh up the respective rights and risks to assess whether or not we can disclose those CCTV images. All Rights requests will be responded to and overseen by our Data Compliance Officer, and in any complex cases they may seek external legal advice.

There are very specific exemptions or partial exemptions for some of these Rights and not all of them are absolute rights. However the right to not receive marketing material or to withdraw a previously given consent are absolute rights, so they should be complied with immediately.

Where an individual considers that we have not complied with their Rights request e.g. exceeded the time period, they can seek a court order and compensation. If the court agrees with the individual, it will issue a court order, to make us comply. The court

can also award compensation. They can also complain to the regulator for privacy legislation, which in our case will usually be the ICO.

In addition to the rights discussed in this document, any person may ask the ICO to assess whether it is likely that any processing of personal data has or is being carried out in compliance with the privacy legislation. The ICO must investigate and may serve an "Information Notice" on us (if we are the relevant controller). The result of the investigation may lead to an "Enforcement Notice" being issued by the ICO. Any such assessments, information notices or enforcement notices should be sent directly to our Data Compliance Officer from the ICO.

In the event of a member of staff receiving such a notice or other correspondence from the ICO, they must immediately pass the communication to our Data Compliance Officer.

Notification and response procedure

If a member of staff has a request or believes they have a verbal request for the exercise of a Right, they should:

- pass the call to their manager. The manager should take and record all relevant details and explain the procedure.
- if possible try to get the request confirmed in writing addressed to the Data Compliance Officer;
- inform our Data Compliance Officer of the request; and
- our Data Compliance Officer will then respond to the data subject on our behalf.

If a letter or fax exercising a Right is received by any member of staff they should:

- pass the letter to their manager;
- the manager must log the receipt of the correspondence with our Data Compliance Officer and send a copy of it to them; and
- our Data Compliance Officer will then respond to the data subject on our behalf.

If an email exercising a Right is received by any member of staff they should:

- pass the email to their supervisor/manager;
- the manager must log the receipt of the email with our Data Compliance Officer and send a copy of it to them; and
- our Data Compliance Officer will then respond to the data subject on our behalf.

Our Data Compliance Officer will co-ordinate our response to any Rights request, taking external legal advice where necessary. The action taken will depend upon the nature of the Rights request. The Data Compliance Officer will write to the individual and explain the legal situation and whether we will comply with the Rights request. A standard letter/email from the Data Compliance Officer should suffice in most cases.

The Data Compliance Officer will inform the relevant management line of any action that must be taken to legally comply. The manager/senior manager who receives the Rights request will be responsible for ensuring that the relevant response is made within the time period required.

The Data Compliance Officer will co-ordinate any additional activity required by the IT Department to meet the Rights request.

The Data Compliance Officer's reply will be validated by the relevant manager of the department producing the response. For more complex cases, the letter/email to be sent will be checked by external legal advisors.

Your main obligations

What this all means for you can be summarised as follows:

- Treat all personal data with respect;
- Treat all personal data how you would want your own personal data to be treated;
- Immediately notify your line manager or the Data Compliance Officer if any individual says or does anything which gives the appearance of them wanting to invoke any Rights in relation to personal data relating to them;
- Take care with all personal data and items containing personal data you handle or come across so that it stays secure and is only available to or accessed by authorised individuals; and

- Immediately notify the Data Compliance Officer if you become aware of or suspect the loss of any personal data or any item containing personal data. For more details on what to do in the event of a data breach, please see our separate Data Breach Policy which applies to all our staff regardless of their position or role in our organisation

Your activities

Data protection laws have different implications in different areas of our organisation and for different types of activity, and sometimes these effects can be unexpected.

Areas and activities particularly affected by data protection law include human resources, payroll, security (e.g. CCTV), customer care, sales, marketing and promotions, health and safety and finance.

There are also additional rules applicable to carrying out electronic marketing under regulations commonly referred to as the Privacy and Electronic Communication Regulations or PECR. Electronic marketing will cover sending marketing or promotional emails/texts or makes marketing telephone calls. Essentially we need to have obtained the specific informed consent of the data subject to receiving electronic marketing from us for each channel we use before we are able to send them marketing and promotional materials via that channel. Sales and marketing teams have separate rules and policies to make sure that they comply with this area of law.

You must consider what personal data you might handle, consider carefully what data protection law might mean for you and your activities, and ensure that you comply at all times with this policy.

Practical matters (Dos and Don’ts)

Whilst you should always apply a common sense approach to how you use and safeguard personal data, and treat personal data with care and respect, set out below are some examples of dos and don’ts:

- Do not take personal data out of the organisation’s premises (unless absolutely necessary).

- Only disclose your unique logins and passwords for any of our IT systems to authorised personnel (e.g. IT) and not to anyone else.
- Never leave any items containing personal data unattended in a public place, e.g. on a train, in a café, etc and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.
- Never leave any items containing personal data in unsecure locations, e.g. in car on your drive overnight (this would include paper files, mobile phone, laptops, tablets, memory sticks etc).
- If you are staying at a hotel then utilise the room safe or the hotel staff to store items containing personal data when you do not need to have them with you.
- Do encrypt laptops, mobile devices and removable storage devices containing personal data.
- Do lock laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use.
- Do password protect documents and databases containing personal data.
- Never use removable storage media to store personal data unless the personal data on the media is encrypted.
- When picking up printing from any shared printer always check to make sure you only have the printed matter that you expect, and no third party's printing appears in the printing.
- Do use confidential waste disposal for any papers containing personal data, do not place these into the ordinary waste or place them in a bin or skip etc. Either use a confidential waste service or have them shredded before placing them in the ordinary waste disposal.
- Do dispose of any materials containing personal data securely, whether the materials are paper based or electronic.
- When in public place, e.g. a train or café, be careful as to who might be able to see the information on the screen of any device you are using when you have personal information on display. If necessary move location or change to a different task.
- Do ensure that your screen faces away from prying eyes if you are processing personal data, even if you are working in the office. Personal data should only be accessed and seen by those who need to see it.

- Use a screen lock on your laptop or tablet when you are not actually working on it.
- Make sure any wi-fi is secure and use a virtual private network and the authentication and log in methods approved by our IT team when logging onto work from a public place. It will be preferable to use your work mobile phone as a wi-fi hotspot rather than use a public wi-fi network.
- Do challenge unexpected visitors or employees accessing personal data.
- Do not leave personal data lying around, store it securely whether working in the office.
- When speaking on the phone in a public place, take care not to use the full names of individuals or other identifying information, as you do not know who may overhear the conversation. Instead use initials or just first names to preserve confidentiality.
- If taking down details or instructions from a customer in a public place when third parties may overhear, try to limit the information which may identify that person to others who may overhear in a similar way to if you were speaking on the telephone.
- Use headphones for conversations rather than loudspeakers.

Homeworking practical matters (Dos and Don'ts)

Working from home brings its own risks. Whilst you might assume your home is not a public place, often from a data protection perspective it is. For example other members of your household are not entitled to access to personal data you may process whilst working at home or they may overhear conversations you are involved in which reference or disclose personal data.

- Treat your home as though it were a public place for the purposes of homeworking. This includes your garden as well as inside your home.
- Make sure your home wi-fi is secure and use a virtual private network and the authentication and log in methods approved by our IT team when logging onto work from your home.

- When speaking on the phone at home when other members of your household may overhear, take care not to use the full names of individuals or other identifying information, as you do not know who may overhear the conversation. Instead use initials or just first names to preserve confidentiality. This will always be the case when in your garden.
- If taking down details or instructions from a customer when at home when third parties may overhear, try to limit the information which may identify that person to others who may overhear in a similar way to if you were speaking on the telephone.
- Use headphones for conversations rather than loudspeakers.
- Do ensure that your screen faces away from prying eyes if you are processing personal data, even if you are working in your home. Personal data should only be accessed and seen by those who need to see it. So set up your workstation so you have your back to a wall if possible.
- Use a screen lock on your laptop or tablet when you are not actually working on it.
- If working from home either bring any papers containing personal data into the office for disposal into the confidential waste disposal or shred them at home before placing them in the ordinary waste disposal. Do not place them in your ordinary household waste in non-shredded form.
- Do not leave personal data lying around, store it securely when working from home.
- Only take home any personal data you need to have access to in order to perform your work. It is safer to access personal data by accessing the work IT system rather than printing physical copies and taking them home.
- Only take home any personal data you need to have access to in order to perform your work. It is safer to access personal data by accessing the work IT system rather than printing physical copies and taking them home.
- Never leave any items containing personal data in unsecure locations, e.g. lying on your workstation overnight (this would include paper files, mobile phone, laptops, tablets, memory sticks etc). Aim to pack them away in a locked area where possible when you do not need access to them or at the very least make sure they are put away out of sight of the other members or your household.

- Stress to other members of your household that your work and work materials are private.

Security practical matters (Dos and Don'ts)

- Never act on instructions from someone unless you are absolutely sure of their identity, and if you are unsure then take steps to determine their identity. This is particularly so where the instructions relate to information which may be sensitive or damaging if it got into the hands of a third party or where the instructions involve money, valuable goods or items or cannot easily be reversed.
- Do not transfer personal data to any third party without prior written consent of your line manager or our Data Compliance Officer.
- **Do notify your line manager or our Data Compliance Officer immediately of any suspected or actual security breaches.**
- **If any personal data is lost, or any devices or materials containing any personal data are lost, or you suspect that they may have been, report it immediately to our Data Compliance Officer.**
- **For more details on what to do in the event of a data breach, please see our separate Data Breach Policy which applies to all our staff regardless of their position or role in our organisation**.

However you should always take a common sense approach, and if you see any areas of risk that you think are not addressed or you become aware of or suspect any issues relating to data protection then please bring it to the attention of our Data Compliance Officer

Foreign transfers of personal data

Croudace Homes Group is not currently aware of any personal data processed by the Company that is transferred outside of the UK, the European Union (EU) or the European Economic Area (EEA). Note that since Brexit the UK is no longer part of the EU or EEA. However the EU and the EEA have been approved by the ICO as countries with adequate protections in place to protect personal data and likewise the EU and EEA have approved the UK as having adequate protections in place to protect

personal data. This means that subject to appropriate contracts or arrangements being put in place personal data can be transferred to and from these jurisdictions though this will generally not be required in relation to our business as most of our personal data is only processed in the UK.

However personal data must not be transferred outside the UK/EU/EEA unless the destination country ensures an adequate level of protection for the rights of the data subject in relation to the processing of personal data or we put in place adequate protections.

These adequate protections may come from special detailed contracts we need to put in place with the recipient of the personal data, with them agreeing to be bound by specific data protection rules under standard forms of contract approved by the ICO or EU Commission (with amendments approved by the ICO) or due to the fact that the recipient's own country's laws provide sufficient protection for personal data.

These restrictions also apply to transfers of personal data outside of the UK/EU/EEA even if the personal data is not being transferred outside of our group of companies.

You must not under any circumstances transfer any personal data outside of the UK/EU/EEA without your line manager's or the Data Compliance Officer's prior written consent. Even for transfers from the UK to the EU/EEA you should have the Data Compliance Officer confirm that the required contracts or arrangements are in place to permit that transfer, though they are likely to need to be less detailed than those that would need to be in place to transfer personal data outside of the UK/EU/EEA.

We will also need to inform data subjects of any transfer of their personal data outside of the UK and may need to amend their privacy notice to take account of the transfer of data whether it is transferred inside or outside of the UK/EU/EEA.

If you are involved in any new processing of personal data which may involve transfer of personal data outside of the UK then please seek approval of your line manager or our Data Compliance Officer prior to implementing any processing of personal data which may have this effect.

Queries

If you have any queries about this Policy please contact either your line manager or the Data Compliance Officer (e-mail gdpr@croudace.co.uk) .