Custodian Property Income REIT Plc

Data Protection Policy

Our Policy

Custodian Property Income REIT Plc (**CREIT**) 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. This policy is applicable to the Directors and Officers of CREIT and also the staff of any sub-contractors or sub-processors for CREIT.

References in this Policy to "**us**", "**we**" and "**our**" are to CREIT and references to "**you**", "**your**" and "**yourself**" are references to Directors and Officers of CREIT or staff of any sub-contractors or sub-processors of CREIT.

We recognise that you have an important role to play in achieving these aims. 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.

Compliance with data protection requirements is overseen and enforced in the UK by the Information Commissioner's Office (**ICO**). The ICO has extensive powers in relation to ensuring compliance with data protection requirements.

If at any time you have any queries on this Policy, your responsibilities or any aspect of data protection law, seek advice. Contact the Data Protection Officer of the Investment Manager (**DPO**) or CREIT's Company Secretary.

1. Who is responsible for data protection?

1.1 The Directors and Officers and the staff of those who process personal data on our behalf are responsible for data protection, and each person has their role to play to make sure that we are compliant with data protection laws.

1.2 We are not required to appoint a Data Protection Officer. The DPO is responsible for overseeing our compliance with data protection laws.

2. Why do we have a data protection policy?

2.1 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.

2.2 This Policy works in conjunction with other policies implemented by us from time to time.

3. **Status of this Policy and the implications of breach.**

3.1 Any breaches of this Policy will be viewed very seriously. All Directors and Officers and key staff of our sub-contractors or sub-processors must read this Policy carefully and make sure they are familiar with it. Breaching this Policy is a disciplinary offence.

3.2 If you are a member of staff of one of our sub-contractors or sub-processors, then breach of this policy is likely to be a disciplinary offence to be dealt with by your employer, and in addition you will place the contract between us and your employer at risk.

3.3 If you do not comply with Data Protection Laws and/or this Policy, then you are encouraged to report this fact immediately to the DPO at info@custodiancapital.com. 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.

3.4 Also if you are aware of or believe that any other staff or a representative of ours is not complying with Data Protection Laws and/or this Policy you should report it in confidence to the DPO at info@custodiancapital.com. The Investment Manager's Whistleblowing Procedure will apply in these circumstances and you may choose to report any non-compliance or breach through our confidential whistleblowing reporting facility.

4. **Other consequences**

4.1 There are a number of serious consequences for both yourself and us if we do not comply with Data Protection Laws. These include:

4.1.1 For you:

4.1.1.1 **Disciplinary action:** Your terms require you to comply with our policies and if you work for one of our sub-contractors or sub-processors the same is likely to apply. Failure to do so could lead to disciplinary action including dismissal.

4.1.1.2 **Criminal sanctions:** Serious breaches could potentially result in criminal liability.

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

4.1.2 For CREIT or its sub-contractors and sub-processors:

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

4.1.2.2 **Civil Fines:** These can be up to £17 million or 4% of group worldwide turnover whichever is higher.

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

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

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

4.1.2.6 **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.

4.1.2.7 **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 and disregarding our legal obligations.

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

4.1.3 For CREIT's sub-contractors and sub-processors and their staff:

4.1.3.1 In addition to the risks outlined above the contract between CREIT and the sub-contractor or sub-processor is likely to have been breached which may lead to a claim for damages.

4.1.3.2 The contract between CREIT and the sub-contractor or sub-processor may be terminated due to breach.

5. Data protection laws

5.1 The Data Protection Act 2018 (**DPA 2018**) and the General Data Protection Regulation as adopted by the UK (**UK GDPR**) and other laws relating to data protection matters apply to any personal data that we process. These are together referred to as the **Data Protection Laws**. The UK GDPR originates from European data protection law that has been adopted by the UK after Brexit. The DPA 2018 is the UK's own data protection law that sits alongside the UK GDPR.

5.2 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).

6. Key words in relation to data protection

6.1 **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).

6.2 **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).

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

6.4 **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 or destruction of personal data, including CCTV images.

6.5 **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 Directors and Officers and generally we will be a controller of personal data relating to investors in our funds, our shareholders and our tenants of any properties we own.

6.6 **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.

7. **Personal data**

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

7.1.1 identifies the individual. For instance, names, addresses, telephone numbers and email addresses;

7.1.2 its content is about the individual personally. For instance, medical records, credit history, investment records, a recording of their actions, or contact details;

7.1.3 relates to property of the individual, for example property they rent from us, their home, their car or other possessions;

7.1.4 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);

7.1.5 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 meeting this may not relate to the individual and may be more likely to relate to the company they represent;

7.1.6 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 he was involved in. For instance, if a work meeting is to discuss the individual's performance this is likely to relate to the individual;

7.1.7 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;

7.1.8 is an expression of opinion about the individual; or

7.1.9 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).

7.2 Information about companies or other legal persons who are not living individuals is not personal data. However, information about directors, shareholders, officers and employees, and about sole traders or partners, is usually personal data, so business related information can often be personal data.

7.3 Examples of information likely to constitute personal data:

7.3.1 Unique names;

7.3.2 Names together with email addresses or other contact details;

7.3.3 Job title and employer (if there is only one person in the position);

7.3.4 Information about individuals obtained as a result of Anti Money Laundering checks or credit checks;

7.3.5 Investor profile information (e.g. preferences); and

7.3.6 Financial information and accounts (e.g. information about investments, tax liabilities, income, expenditure, credit history).

8. Lawful basis for processing

8.1 For personal data to be processed lawfully, we must be process it on one of the legal grounds set out in the Data Protection Laws.

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

8.2.1 the data subject has given their consent to the processing;

8.2.2 the processing is necessary for the performance of a contract with the data subject;

8.2.3 the processing is necessary for the compliance with at legal obligation to which the controller is subject; or

8.2.4 the processing is necessary the legitimate interest reasons of the controller or a third party.

9. Special category data

9.1 Special category 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.

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

9.3 To lawfully process special categories of personal data we must also ensure that either the individual has given their explicit consent to the processing or that another of the following conditions has been met:

9.3.1 the processing is necessary for the performance of our obligations under employment law;

9.3.2 the processing is necessary to protect the vital interests of the data subject. The ICO has previously indicated that this condition is unlikely to be met other than in a life or death or other extreme situation;

9.3.3 the processing relates to information manifestly made public by the data subject;

9.3.4 the processing is necessary for the purpose of establishing, exercising or defending legal claims; or

9.3.5 the processing is necessary for the purpose of preventative or occupational medicine or for the assessment of the working capacity of the employee.

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

9.4.1 ensure that either the individual has given their explicit consent to the processing; or

9.4.2 ensure that our processing of those criminal records history is necessary under a legal requirement imposed upon us.

9.5 We would normally only expect to process special category personal data or criminal records history data usually in a Human Resources context and also in the context of our investors to comply with money laundering checks under legal and regulatory obligations placed on us.

10. **When do we process personal data?**

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

10.2 Examples of processing personal data might include:

10.2.1 Using personal data to correspond with investors or shareholders;

10.2.2 Holding personal data in our databases or documents; and

10.2.3 Recording personal data in personnel or investor files.

11. **Outline**

11.1 The main themes of the Data Protection Laws are:

11.1.1 good practices for handling personal data;

11.1.2 rights for individuals in respect of personal data that data controllers hold on them; and

11.1.3 being able to demonstrate compliance with these laws.

11.2 In summary, Data Protection Laws requires each controller to:

11.2.1 only process personal data for certain purposes;

11.2.2 process personal data in accordance with the 6 principles of 'good information handling' (including keeping personal data secure and processing it fairly and in a transparent manner);

11.2.3 provide certain information to those individuals about whom we process personal data which is usually provided in a privacy notice, for example you will have received one of these from your employer;

11.2.4 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

11.2.5 keep adequate records of how data is processed and, where necessary, notify the ICO and possibly data subjects where there has been a personal data breach.

11.3 It is your responsibility to familiarise yourself with this Policy.

12. Data protection principles

12.1 The Data Protection Laws, in Article 5 of UK GDPR sets out 6 principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:

12.1.1 processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met ("lawfulness, fairness and transparency");

12.1.2 collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("purpose limitation");

12.1.3 adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation");

12.1.4 accurate and where necessary kept up to date ("accuracy");

12.1.5 kept for no longer than is necessary for the purpose ("storage limitation");

12.1.6 processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and confidentiality").

12.2 There is also a requirement, as well as being compliant, to be able to demonstrate compliance with Data Protection Laws with various records, procedures and policies ("accountability").

13. Data subject rights

13.1 Under Data Protection Laws individuals have certain rights (**Rights**) in relation to their own personal data. In summary these are:

13.1.1 The right to withdraw any consent they have given in relation to the use of their personal data;

13.1.2 The rights to access their personal data, usually referred to as a subject access request;

13.1.3 The right to have their personal data rectified;

13.1.4 The right to have their personal data erased, usually referred to as the right to be forgotten;

13.1.5 The right to restrict processing of their personal data;

13.1.6 The right to object to receiving direct marketing materials;

13.1.7 The right to portability of their personal data;

13.1.8 The right to object to processing of their personal data; and

13.1.9 The right to not be subject to a decision made solely by automated data processing.

13.2 The exercise of these Rights may be made in writing, including email, and also verbally and should be responded to in writing 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.

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

13.4 If we are unsure about the identity of the individual exercising the Rights, then we will need to take steps to ensure we verify their identity so that we know they are the individual they claim to be and therefore are entitled to exercise Rights in relation to their personal data.

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

13.6 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 consent are absolute rights, so they should be complied with immediately.

13.7 Where an individual considers that we have not complied with their request e.g. exceeded the time limits, 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.

13.8 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 from the ICO should be sent immediately to the DPO at info@custodiancapital.com.

14. Notification and response procedure

14.1 If you receive a verbal request, letter, fax or e-mail for the exercise of a Right or any complaint regarding personal data, you should immediately inform the DPO and pass them all relevant information.

14.2 If you are aware of any data subject invoking any of their Rights in relation to their personal data, or any other issue being raised in relation to their personal data (e.g. a complaint) then it is important the above notification is carried out very quickly as time limits apply to dealing with Rights apply and if can be difficult to comply with these time limits even where we immediately become aware of the position.

14.3 The DPO will co-ordinate our response which may include written material provided by external legal advisors. The action taken will depend upon the nature of the request. The DPO will usually write to the individual and explain the legal situation and explain how we will comply with the request.

14.4 The DPO will co-ordinate any additional activity required by the IT Department to meet the request.

14.5 The DPO will be responsible for ensuring that the relevant response is made within the time period required.

14.6 The DPO's reply will be validated by the relevant manager of the Investment Manager. For more complex cases, the letter/email to be sent will be checked by external legal advisors.

15. Your main obligations

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

15.1.1 Treat all personal data with respect;

15.1.2 Treat all personal data how you would want your own personal data to be treated;

15.1.3 Immediately notify the DPO if any individual says or does anything which gives the appearance of them wanting to invoke any Rights or raise a complaint in relation to personal data relating to them;

15.1.4 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

15.1.5 Immediately notify the DPO if you become aware of or suspect the loss of any personal data or any item containing personal data. For more details on this see the section below on personal data breaches.

16. Your activities

16.1 Data protection laws have different implications for different types of activity, and sometimes these effects can be unexpected.

16.2 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.

16.3 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.

17. Practical matters

17.1 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:

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

17.1.2 Only disclose your unique logins and passwords for any of our IT systems to authorised personnel (e.g. IT) and not to anyone else.

17.1.3 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.

17.1.4 Never leave any items containing personal data in unsecure locations, e.g. in car on your drive overnight and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.

17.1.5 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.

17.1.6 Do encrypt laptops, mobile devices and removable storage devices containing personal data.

17.1.7 Do lock laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use.

17.1.8 Do password protect documents and databases containing personal data.

17.1.9 Never use removable storage media to store personal data unless the personal data on the media is encrypted.

17.1.10 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.

17.1.11 Use confidential waste disposal for any papers containing personal data, do not place these into the ordinary waste, place them in a bin or skip etc, and either use a confidential waste service or have them shredded before placing them in the ordinary waste disposal.

17.1.12 Do dispose of any materials containing personal data securely, whether the materials are paper based or electronic.

17.1.13 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.

17.1.14 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.

17.1.15 Do challenge unexpected visitors or employees accessing personal data.

17.1.16 Do not leave personal data lying around, store it securely.

17.1.17 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.

17.1.18 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.

17.1.19 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.

17.1.20 Do not transfer personal data to any third party without prior written consent of the DPO.

17.1.21 Notify the DPO immediately of any suspected security breaches or loss of personal data.

17.1.22 If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to the DPO. For more details on this see the section below on personal data breaches.

17.1.23 If you are working remotely make sure you follow our IT security procedures.

17.1.24 If you are working from home, whether inside your home or in your garden, this is effectively a public place as other members of your household may see or overhear personal data. Treat working at home or in your garden in the same way as if you were working in a public place, e.g. in a café or on a train, and take exactly the same precautions.

17.2 However you should always take a common sense approach, and if you see any areas of risk that you think are not addressed then please bring it to the attention of the DPO.

18. Foreign transfers of personal data

18.1 Personal data must not be transferred outside the UK/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.

18.2 These protections may come from special contracts we need to put in place with the recipient of the personal data, from them agreeing to be bound by specific data protection rules or due to the fact that the recipients own country's laws provide sufficient protection.

18.3 These restrictions also apply to transfers of personal data outside of the UK/EEA even if the personal data is not being transferred by us but by one of our sub-contractors or sup-processors.

18.4 You must not under any circumstances transfer any personal data outside of the UK/EEA without your line manager's or the DPO's prior written consent.

18.5 We will also need to inform data subjects of any transfer of their personal data outside of the UK/EEA and may need to amend their privacy notice to take account of the transfer of data outside of the UK/EEA.

18.6 If you are involved in any new processing of personal data which may involve transfer of personal data outside of the UK/EEA, then please seek approval of your

line manager or our DPO prior to implementing any processing of personal data which may have this effect.

19. Personal data breaches

19.1 This part of Policy covers what are commonly referred to as personal data breaches or data breaches. This includes any loss of data owned or used by us, whether a third party obtains access to the data or not. We approach all data breaches in essentially the same way, whether or not they involve personal data. So for example a data breach will include:

19.1.1 Loss of a computer, laptop, mobile telephone or removable storage media.

19.1.2 Loss of our data stored on a computer or server due to corruption of the hard drive.

19.1.3 Erasure of data which should not have been erased.

19.1.4 Loss of physical papers or files containing our data.

19.1.5 Hacking of our computer network and systems or a computer network and system that processes data for us.

19.1.6 A ransomware, malware, virus or other malicious code attack made to our computer network and systems.

19.1.7 Non-secure destruction of our data.

19.1.8 Sending an email or post to the wrong person which contains our data.

19.1.9 Sending an email to a group of recipients using the "to" or “cc” field when their email addresses should not have been disclosed to the other recipients.

19.1.10 Allowing someone to overhear a telephone conversation when identifying details are disclosed.

19.1.11 Data being disclosed or revealed to someone else in the organisation who is not entitled to see or know that data.

19.2 The above is not an exhaustive list, and data losses and breaches can take many forms. It also applies if the events occur in relation to our data which is held by a sub-contractor or processor of ours.

19.3 If anything occurs or involves loss of our data or unauthorised third party access to our data then it will be a data breach. For the rest of this Policy we have used the term “data breach or loss” as this is less confusing and better describes what a data breach is. We also require reporting of data breaches or losses, whether or not the data relates to an individual, so any type of data breach or loss involving our data should be reported to us.

19.4 Compliance with our policies on security, IT security 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.

20. **What you must do if you become aware of a data breach or loss**

20.1 As soon as you become aware of any data breach or loss which involves our data, or any data we process on behalf of anyone else, you must IMMEDIATELY notify the DPO by email at info@custodiancapital.com or by telephone on 0116 240 8700. You must also make sure that receipt of the notification is acknowledged, this is to guard against the recipient being out of the office or on holiday. If you do not get an acknowledgement within 24 hours then immediately let the Company Secretary know about the data breach or loss.

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

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

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

20.5 We will treat all notifications which are about a colleague or another worker in confidence in accordance with the Investment Manager's whistleblowing policy.

21. **Failure to notify a data breach or loss to us**

21.1 If you notify a data breach or loss in accordance with this Policy, then even if you are at fault in causing or contributing to the data breach or loss, for example due to human error, then we would prefer to know about the data breach or loss. The fact that you have reported it will work in your favour, and it is a fact of life that data breaches or losses sometimes occur, often due to human error or the need to improve our systems and procedures.

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

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

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

22. **Why you must notify us of a data breach or loss**

22.1 Under Data Protection Laws we are under a duty to inform the ICO of data breaches or losses involving personal data which we control as soon as possible in cases where the data breach or loss may result in harm to individuals.

22.2 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 breach or loss in

accordance with this Policy. The time period also runs during non-working hours, during bank holidays and weekends. Therefore the notification to us in accordance with this Policy must be made immediately.

22.3 Your notification will allow us to assess whether or not we need to notify the ICO regarding the data loss. It will also allow us to respond quickly to mitigate or remedy the position. The longer between the data breach or loss and you notifying us of the data breach or loss the harder it becomes to mitigate or remedy the data breach or loss.

22.4 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 breach or loss which you are aware of is treated as serious misconduct, and could result in dismissal or termination of a contract.

22.5 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 breach or 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.

23. WHAT HAPPENS ONCE YOU HAVE NOTIFIED

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

23.2 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 breach or loss to the ICO.

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

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

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

23.6 Whatever happens we will record the data breach or loss on the Investment Manager's data breach 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 breaches or losses.

Ends