GUIDANCE NOTE F03
GENERAL DATA PROTECTION REGULATION

Revised — May 2018

ARMA Standards

The Standards have been written to apply to residential long leasehold properties (a lease of a term in excess of 21 years when originally granted) in England and Wales where a service charge, which varies according to expenditure, is payable.

They represent the core of good practice for managing agents. We believe they are achievable by any well-run company. The applicable (if any) Standards related to this Guidance Note are stated below.

Standards in RED: An obligation to adhere to the Standard

Standards in GREEN: An obligation to adhere to the Standard unless there is a justifiable reason not to comply that the Managing Agent must be able to demonstrate

6.2 Statutory Compliance

The Managing Agent Must have regard to and comply with:

c) legislation relating to data protection.

Guidance Note Contents

Overview

1. **All managing agents have legal obligations under the General Data Protection Regulation (GDPR) and must adhere to the general principles set down by the GDPR.**

   - **You will have to notify the Information Commissioner (ICO) of your data processing activity.**
   - **Managing agents must maintain records of their processing activities.**
   - **Managing agents must have a purpose for processing personal data and a valid lawful basis for processing personal data.**
   - **All data subjects (i.e. individuals) have rights under the GDPR. These rights include:**

     - right to be informed
     - right of access (commonly known as subject access requests)
     - right to rectification
     - right to erasure

   - **Managing agents must maintain records of any incidents of personal data breach, and, where appropriate, notify any breach to the ICO and/or data subject.**
   - **This Guidance Note answers some frequently asked questions about GDPR and data protection.**

Overview

On 25th May 2018, the European Union's General Data Protection Regulation (GDPR), arguably the biggest shake up of data protection rules in 25 years, came into force.

Data protection has become the cornerstone of your organisation's policy and procedures, as the quote from the ICO below highlights:

"The new law equals bigger fines for getting it wrong but it is important to recognise the business benefits of getting data protection right. There is a real opportunity for organisations to present themselves on the basis of how they respect the privacy of individuals, and gain a competitive edge. But if your organisation can't demonstrate that good data protection is a cornerstone of your business policy and practices when the new law comes in [this] year, you're leaving your organisation open to enforcement action that can damage both public reputation and bank balance".

Data protection is become the golden thread that weaves through your activities. Your policies and procedures have become living documents; reviewed, updated and amended with regularity. And with regulatory fines of up to €20 million or 4% of global turnover (whichever is the greatest) it's imperative for Managing Agents to comply.

The requirement to comply did not start from 25th May when GDPR came into force. Managing Agents **must** have been compliant by the deadline date of 25th May.

Although there are some similarities between the obligations under the Data Protection Act 1998 (DPA) and GDPR, the GDPR imposes requirements which means that Managing Agents have to demonstrate greater accountability and transparency in relation to the personal data they are processing.

General Principles Of The GDPR

To help understand the requirements of the GDPR, it is helpful to understand the general principles which set out the main responsibilities for organisations under article 5 of the GDPR. Personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes (and not further processed in a manner that's incompatible with those purposes);
- adequate, relevant and limited to what's necessary in relation to those purposes;
- accurate and kept up to date (NB every reasonable step must be taken to ensure that personal data is accurate);
- kept in a form which permits identification of individuals (commonly referred to as data subjects) for no longer than is necessary for the purposes for which their data is being processed; and
- processed in a manner that ensures appropriate security.

As data controllers, Managing Agents are responsible for and must be able to show that they have complied with these principles. Managing Agents will need to demonstrate their compliance. They will do this by:

- implementing appropriate technical and organisational measures that demonstrate compliance (generally in the form of internal data protection policies);
- maintain documentation on processing activities;
- document those processing activities in writing (in a granular way and with links between different pieces of information and different sections in their policies); and
- conduct regular reviews of the personal data they are processing and update their documentation accordingly.

Obligations Of Managing Agents Under The GDPR

- Managing Agents holding personal data on leaseholders demonstrate their compliance with the GDPR principles set out above;
- Managing Agents must notify their details to the Information Commissioner;

- Managing Agents must have a purpose (or purposes) for processing personal data and must document this;
- Managing Agents must have a lawful basis for processing personal data and must document this;
- Managing Agents must describe and document the categories of individuals whose personal data they process and also the categories of personal data they process;
- Managing Agents must document the recipients of the personal data;
- Managing Agents must detail any transfers of personal data to third parties and include details of the transfer mechanism safeguards in place;
- Managing Agents must set out and document their retention schedules regarding personal data;
- Managing Agents must describe and document their technical and organisational security measures in relation to the personal data they are processing;
- Managing Agents must recognise the rights individuals have in relation to their personal data, and will, accordingly, have processes in place in relation to the following:
    I. communicating privacy information;
    II. dealing with subject access requests;
    III. dealing with rectification and accuracy of information held (including requests made by individuals for rectification of any inaccuracies and right to restrict processing);
    IV. handling personal data breaches; and
    V. retention of personal data and erasure.
- Managing Agents will have procedures in place for dealing with data quality reviews in their organisations.

Registration With The ICO

There is an online form to Register or to Renew at www.ico.gov.uk. Registration has to be renewed annually and the ICO will write to you before the expiry date. There are three tiers of fee and controllers are expected to pay between £40 and £2900. The fees are set by Parliament. The tiers depend on the turnover and number of member of staff. Micro organisations (ie those with a maximum turnover of £632,000 or no more than 10 employees) must pay a fee of £40. Small and medium organisations (i.e. those with a maximum turnover of £36 million in a financial year or no more than 250 employees) must pay a fee of £60. It's only if Managing Agents do notfit into either of those categories that the fee payable is £2900.

The GDPR covers computer records and some manual records. You will need to disclose for the process of notification all records that can be easily searched to reveal personal information. Notification is not required for information kept on PLC or limited companies; notification is required for information on partnerships or sole traders.

What Happens If You Fail To Notify?

Failure to notify (or renew) or a failure to pay the correct fee is an offence punishable by a fine of up to £4350 (150% of the top tier fee).

Lawful Bases For Processing Personal Data

The lawful bases for processing under GDPR and broadly similar to the conditions for processing under the Data Protection Act 1988. However, GDPR places a greater emphasis on being accountable for and transparent about your basis for processing personal data. In many cases, the lawful basis for processing will be the same as your existing condition for processing.

The six lawful bases for processing are:

I. **Consent.** This applies where the individual has given clear consent for you to process their personal data for a specific purpose. Bear in mind that consent is withdrawable at any time. Consent is unlikely to be the basis on which Managing Agents process the personal data of leaseholders.
II. **Contract.** This applies where the processing is necessary for a contract that you have with the individual, or because the individual has asked you to take specific

steps before entering into a contract. The likelihood is that Managing Agents will rely on contract as their lawful basis for processing the personal data of leaseholders. Although Managing Agents have no direct contract with leaseholders, they are appointed by the RMCo or the Landlord as their agent, and RMCo or Landlord have a contractual relationship with leaseholder – the lease.

III. **Legal obligation.** This applies where the processing is necessary for you to comply with the law (NB this **does not** include contractual obligations).
IV. **Vital interests.** This applies where the processing is necessary for you to protect someone's life.
V. **Public task.** This applies where the processing is necessary for you to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
VI. **Legitimate interests.** This applies where the processing is necessary for your legitimate interests (or those of a third party), **unless** there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Managing Agents must determine their lawful basis before they start to process personal data. It is important the Managing Agents thoroughly assess upfront which basis is appropriate and document this. It may be possible for more than one basis to apply, depending on the purpose of your processing. If this is the case, you should make this clear at the start.

The accountability principle requires Managing Agents to demonstrate compliance with GDPR, and to have appropriate policies and procedures. This means that Managing Agents will need to show they have properly considered which lawful basis applies to their processing and can justify their decision.

Managing Agents will need to document their decision(s) in their data protection policy and will need to include this information in their privacy notices (See Appendix 3 & 4). Under the transparency provisions of the GDPR, the information you will need to tell leaseholders (and other individuals) includes:

- your intended purpose for processing the personal data; and
- the lawful basis for the processing.

NB this applies whether or not you collect the personal data directly from the individual, or whether you collect their data from another source.

Communicating Information To Leaseholders

A key transparency requirement under GDPR is that individuals are informed about the collection and use of their personal data.

Managing Agents must provide leaseholders with certain information. If the Managing Agent collects the personal data directly from the individual, this information must be provided at the point of collection. If information is collected from other sources (e.g. solicitors) then you must provide the information within a reasonable time and no later than one month.

Managing Agents must actively provide privacy information to leaseholders. Managing Agents can meet this requirement by placing the information on their website, but they must make individuals aware of it and give them an easy way to access it.

Managing Agents may communicate this information by means of a privacy notice. The information provided will include:

- the name and contact details of the Managing Agent;
- the name and contact details of your representative;
- (if you have appointed a Data Protection Officer) the name and contact details of the DPO;
- the purposes of the processing;
- the lawful basis for the processing;
- (if you rely on legitimate interests as your lawful basis) the legitimate interests for the processing;

- (if obtaining data from other sources) the categories of personal data obtained;
- the recipients or categories of recipients of the personal data;
- the details of any transfers of the personal data to any third parties or international organisations;
- the retention periods for the personal data;
- the rights available to individuals in respect of the processing;
- (if you rely on consent as your lawful basis for processing) the right to withdraw consent;
- the right to lodge a complaint with the ICO;
- (if data is obtained from other sources) the source of the personal data;
- the details of whether the individuals are under a contractual or statutory obligation to provide the personal data; and
- (if your processing includes automated decision-making) the details of the existence of automated decision-making, including profiling.

Right Of Access

Leaseholders have a legal right to see the information you hold about them. This right, commonly referred to as subject access, allows individuals to be aware of and verify the lawfulness of your processing.

It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this, and an individual who makes a written request has a right to obtain:

- confirmation that their personal data is being processed;
- access to their personal data; and
- other supplementary information (which largely corresponds to the information that should be provided in a privacy notice).

Under the DPA, Managing Agents had 40 days to respond to a subject access request and could charge a fee of £10.

Under GDPR, the information must be provided without delay and at the latest within one calendar month of receipt.

Managing Agents must provide a copy of the information free of charge. A “reasonable fee” can be charged when a request is manifestly unfounded or excessive, particularly if it’s repetitive.

Managing Agents must verify the identity of the person making the request using “reasonable means”.

If the request is made electronically, you should provide the information in a commonly used electronic format.

Rectification And Accuracy

Under GDPR, leaseholders have the right to have inaccurate personal data rectified. This right links to the accuracy principle. Although Managing Agents may have already taken specific steps to ensure that the personal data of leaseholders was accurate when obtained, this right to rectification imposes a specific obligation on Managing Agents to reconsider the accuracy upon request.

If you receive a request from a leaseholder for rectification of their personal data, you must take reasonable steps to satisfy yourself that the data is accurate and then rectify the data if necessary.

It is important to note that the GDPR does not specify how an individual should make a valid request. Therefore, a leaseholder can make a request for rectification verbally or in writing. It may also be made to anyone in your organisation. You may need to consider which of your staff regularly interact with leaseholders and provide training so that they are able to recognise these type of requests.

Right To Be Forgotten

GDPR introduces a new right for individuals to have personal data erased. This is commonly referred to as the right to be forgotten.

The right to be forgotten applies in certain circumstances, including if the personal data is no longer necessary for the purpose for which you originally collected or processed it.

It is important to note that the GDPR does not specify how an individual should make a valid request. Therefore, a leaseholder can make a request for erasure verbally or in writing. It may also be made to anyone in your organisation. You may need to consider which of your staff regularly interact with leaseholders and provide training so that they are able to recognise these type of requests.

Security Principle

A key principle of GDPR is that personal data is processed securely by means of "appropriate technical and organisational measures". This mirrors the previous requirement under DPA.

Article 5(1)(f) concerns "integrity and confidentiality" of personal data. Accordingly, Managing Agents must process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

Managing Agents must have appropriate security in place to prevent the personal data they hold from being accidentally or deliberately compromised.

The security principle goes beyond the way Managing Agents store or transmit information. Every aspect of your processing of personal data is covered. This means that Managing Agents should put in place security measures which ensure that:

- data can be accessed, altered, disclosed or deleted only by those authorised to do so;
- the data you hold is accurate and complete in relation to why you are processing it; and
- the data remains accessible and useable (for example if personal data is accidentally lost, you should be able to recover it and prevent any damage or distress to the individuals concerned).

Managing Agents will need to consider and analyse the risks presenting by their processing activities and use this analysis to implement appropriate levels of security. This consideration and analysis will be documented in a Managing Agent's information security policy (or equivalent), and steps will be taken to ensure the policy is implemented.

Those policies will be regularly reviewed and updated where necessary.

Managing Agents will need to ensure their staff understand the importance of protecting personal data and are familiar with your security policy and its procedures.

Personal Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. A breach is about more than just losing personal data.

Some examples of personal data breaches include:

- access by an unauthorised third party;
- sending personal data to the wring recipient;
- devices containing personal data being lost or stolen; or

- loss of availability of personal data.

Where a personal data breach has occurred, Managing Agents will need to establish the likelihood and severity of the resulting risk to individual's rights and freedoms.

If it's likely to result in a risk to people's rights and freedoms, then the Managing Agent must notify the ICO. The notification must be made without undue delay and within 72 hours of becoming aware.

If it's likely to result in a high risk to people's rights and freedoms, then the individual(s) concerned must be notified without undue delay.

If the breach is not likely to result in a risk (or high risk) to people's rights and freedoms, then there is no requirement to notify. However, Managing Agents will need to document their decisions in the event no notification is made. All breaches should be recorded, regardless of whether or not they need to be reported to the ICO.

Appendix II provides for a Data Breach Reporting Flowchart that may assist Managing Agents in their approach.

Failing to notify can result in a significant fine of up to €10 million or 2% of your global turnover, whichever is the greater.

A Landlord's Legal Obligation To Disclose Information

The GDPR will not prevent a landlord from releasing personal information where they have a legal obligation to do so. For example, under S22 of the Landlord and Tenant Act 1985 landlords may have to provide an unedited copy of receipts and invoices which make up the service charge accounts to a leaseholder if he or she asks for it. If so, the landlord will have to comply with the request even if it means revealing information about other leaseholders.

Can I Provide Names And Addresses Of Leaseholders To Other Leaseholders In The Block?

Generally you should not disclose information to a third party unless the individual concerned has been informed about the disclosure. There are public records of such information that any leaseholder can check including Land Registry and electoral registers. It follows therefore, that in any accounts you produce the most you should show is the flat/unit number.

Can Landlords Put Up A List Of Leaseholders Who Are in Arrears?

No. Where a leaseholder leaves without paying and without making any arrangement to pay, landlords may provide their details to a tracing agent or debt collection company to help them recover money owed to them. However, it would be good practice to make leaseholders aware that in such circumstances this will happen.

Can Landlords Display Details Of A Leaseholder Who Left Without Paying The Rent Or Service Charge?

Where a leaseholder leaves without paying and without making any arrangement to pay, landlords may provide their details to a tracing agent or debt collection company to help them recover money owed to them. However, it would be good practice to make leaseholders aware that in such circumstances this will happen.

What About Handing Over Records When Transfers Of Management Occur?

Managing agents are advised to seek a written assurance from the new managing agent (or RTMC) that they will process the data handed over according to the GDPR.

What About Pitching For New Management Business?

Managing Agents are advised to include a statement about GDPR in their information about their business - that leaseholders' and other personal data will be processed for the effective management of the property. Set out what data is needed to be held, what it will be used for and how it will be kept secure.

Data Destruction And Shredding

How do you dispose of paper waste, hard drives, CDs? The GDPR requires you to dispose and destroy personal information appropriately. The British Security Industry Association keeps a list of vetted information destruction companies which operate to the relevant British Standard BS8470. View a list of companies at www.bsia.co.uk.

Encryption

There have been a number of reports of laptop computers or discs containing personal information which have been stolen from vehicles, dwellings or left in inappropriate places without being protected adequately. The Information Commissioner has formed the view that in future, where such losses occur and where encryption software has not been used to protect the data, enforcement action will be pursued.

The ICO recommends that portable and mobile devices including magnetic media used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against information being compromised.

Personal information which is stored, transmitted or processed in information, communication and technical infrastructures should also be managed and protected in accordance with the organisation's security policy and using best practice methodologies such as using the International Standard 27001. Further information can be found at https://www.iso.org/isoiec-27001-information-security.html

There are a number of different commercial options available to protect stored information on mobile and static devices and in transmission such as across the Internet.

Encryption software uses a complex series of embedded mathematical algorithms to protect and encrypt information. This process hides the data and prevents any inadvertent access or unauthorised disclosure of information. Since encryption standards are always evolving, it is recommended that data controllers ensure that any solution which is implemented meets the current standard such as the recommended FIPS 140-2 Level 3 approved encryption products.

You can find out more about encryption at the government and business sponsored website www.getsafeonline.org

Requirement For Residential Management Companies To Notify?

The following is the advice received from the Information Commissioner:
With regards to whether Resident Management Companies (RMC) need to notify, this would depend on the individual circumstances of each case and, in particular, whether the resident management company does any processing of personal data itself that the professional management agent does not.

Therefore, in a clear-cut case where all processing of personal data is carried out by the Managing Agent and the RMC does not process any information itself, it is unlikely that the RMC would need to notify as well. However, if the RMC also does some processing of personal data that goes beyond that carried out by the Managing Agent (e.g. a number of residents are unhappy with the behaviour of one of the other residents, and so convene a meeting to decide what to do about it), then the RMC may need to notify as well. The ICO would consider such activities to go beyond the exempt “core business purposes”.

ICO's advice would therefore be that RMC's should speak with the ICO or use their online self-assessment to decide whether they need to notify or not. They do not need to notify with ICO for the activities of any professional Managing Agent that they have contracted (i.e. there is no need for the same processing to effectively be notified twice by two different companies). However, if the RMC carries out its own data processing, it may need to notify for this.

It is also worth noting that the requirement to notify only applies to electronic processing of personal data. Nowadays, it is increasingly common for all processing to be carried out electronically (e.g. notes taken on a laptop, tablet or smartphone). However if all personal data is recorded and held manually and is not put onto a computer or other device at any point (e.g. handwritten meeting minutes stored in a filing cabinet), then there would be no requirement to notify.

Further Information

- The Information Commissioner's Office is at: www.ico.gov.uk or the helpline is 0845 630 6060
- Data Protection Good Practice Note on security of personal information is free from: https://ico.org.uk/
- Data Protection Good Practice Note -Disclosing information about tenants: https://ico.org.uk/
- Vetted and approved data destruction companies can be found at: www.bsia.co.uk/shredding or use the helpline 0845 389 3889
- Encryption advice at: www.getsafeonline.org
- International standard on data security at: https://www.iso.org/isoiec-27001-information-security.html
- GDPR 12-step guidance plan: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

The Association of Residential Managing Agents Ltd
3rd Floor, 2-4 St George's Road
London
SW19 4DP

Tel 020 7978 2607
info@arma.org.uk
www.arma.org.uk

APPENDIX I

GLOSSARY

Biometric Data: Any personal data relating to the physical, psychological or behavioural characteristics of an individual which allows their unique identification.

Consent: Consent is defined as receiving the data subject's agreement to process their data. Agreement must be freely given, informed, specific and unambiguous. Consent can be given in several ways, e.g. via a written statement (including by electronic means) or an oral statement. Gaining consent must be clear and unambiguous. The data subject must understand implicitly what they are providing their data for, how it will be processed, who will process it and how long it will be stored.

Data controller: The entity that determines the purposes, conditions and means of the processing of personal data (so if you are collecting personal data and are determining how it will be processed, you are the controller of that data and must comply with the GDPR).

Data erasure (AKA the right to be forgotten): Entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data.

Data privacy impact assessment (DPIA): A documented assessment of the usefulness, risks and risk mitigation options for a certain type of processing.

Data processor: The entity that processes data on behalf of the data controller. In other words the processor helps a controller by "processing" data based on its instructions, but does not decide what to do with the data.

Data protection officer: An expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set down in the GDPR.

Data subject: A natural person whose personal data is processed by a controller or processor.

Encrypted data: Personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access.

Genetic data: Data concerning the characteristics of an individual which are inherited or acquired which give unique information about the health or physiology of the individual.

Personal data: Any information related to a natural person or "data subject", that can be used directly or indirectly to identify the person (e.g. name, address, IP address etc).

Personal data breach: A breach of security leading to the accidental or unlawful access to, destruction, misuse etc of personal data.

Privacy by design: A principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.

Processing: Any operation performed on personal data, whether or not by automated means, including collection, use, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction etc.

Pseudonymisation: Processing of personal data such that it can no longer be attributed to a single data subject without the use of additional data, so long as the additional data stays separate to ensure non-attribution.

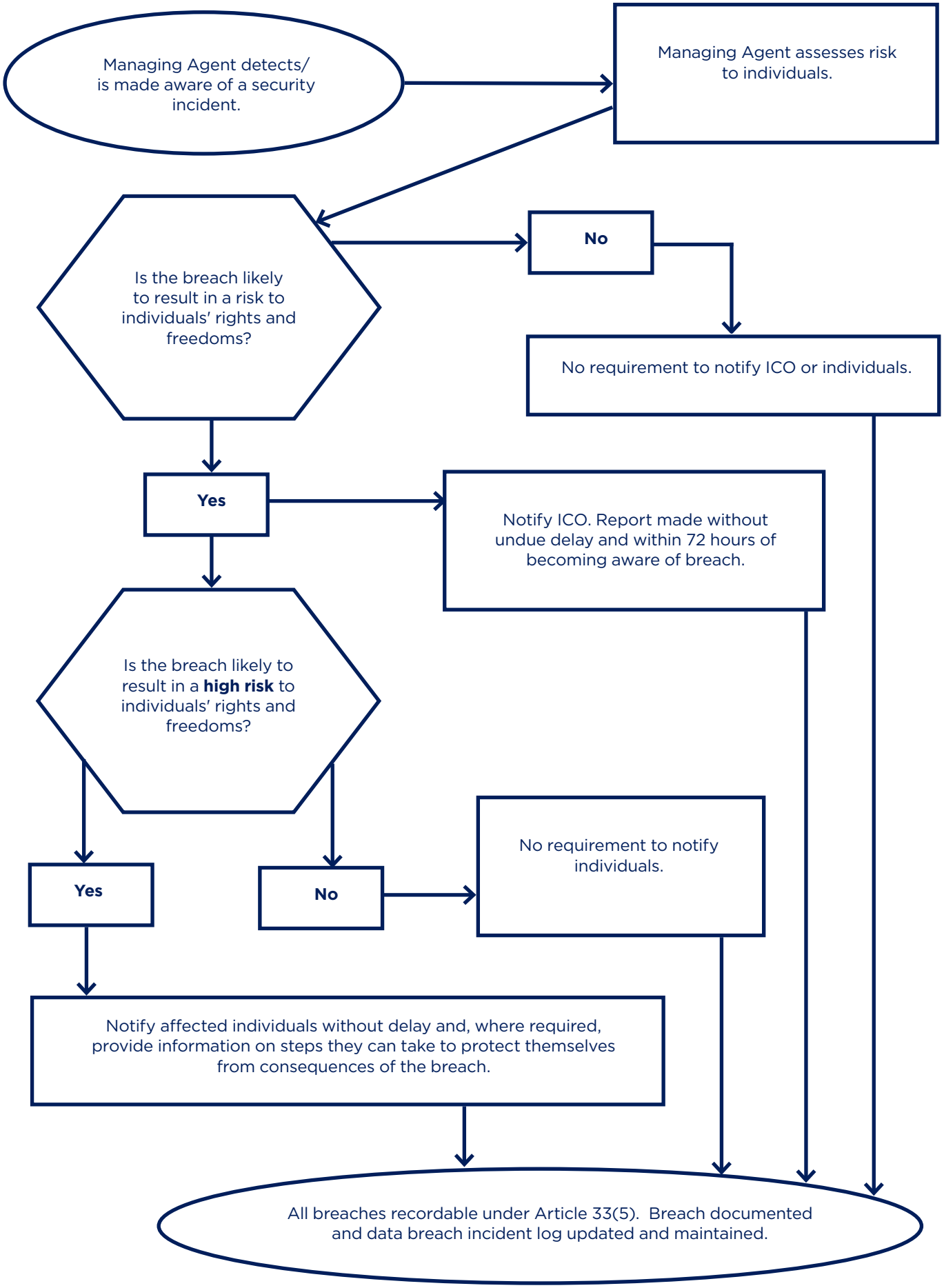
Right to be forgotten (AKA data erasure): Entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data.

Right to access (AKA subject access right): Entitles the data subject to have access to and information about the personal data that a controller has concerning them.

Subject access right (AKA right to access): Entitles the data subject to have access to and information about the personal data that a controller has concerning them.

APPENDIX II

Data Breach Reporting Flowchart



APPENDIX III

PRIVACY NOTICE TEMPLATE

DATED 2018

PRIVACY NOTICE provided by

[insert agent]

This privacy notice explains what personal data (information) we hold about you, how we collect it, and how we use and may share information about you during our management of [INSERT DEVELOPMENT] and after it ends. We are required to notify you of this information under the General Data Protection Regulation.

Please ensure you read this notice (sometimes referred to as a "privacy notice" and any other similar notice we may provide to you from time to time when we collect or process personal information about you. This privacy notice contains important information on who we are, how and why we collect, store, use and share personal information, your rights in relation to your personal information and on how to contact us and supervisory authorities in the event you have a complaint.

1. WHO WE ARE

[INSERT NAME OF AGENT] [trading as [INSERT TRADING NAME, IF DIFFERENT]] collects, uses and is responsible for certain personal information about you. When we do so we are regulated under the General Data Protection Regulation which applies across the European Union (including in the United Kingdom) and we are responsible as 'controller' of that personal information for the purposes of those laws.

In this privacy notice, references to "we" or "us" means [INSERT AGENT]

2. DATA PROTECTION PRINCIPLES

We will comply with the data protection principles when gathering and using personal information, as set out in our GDPR data protection policy.

3. THE PERSONAL INFORMATION WE COLLECT AND USE: INFORMATION COLLECTED BY US

In the course of the performance of our contract as managing agent for the development where you are a leaseholder, [RELEVANT ACTIVITIES] we collect the following personal information when you provide it to us:

- [INSERT DETAILS OF THE PERSONAL DATA YOU WILL COLLECT E.G. NAME, CONTACT DETAILS (ADDRESS, PROPERTY ADDRESS, HOME AND MOBILE TELEPHONE NUMBERS, E-MAIL ADDRESS, MORTGAGE DETAILS ETC)
- [INSERT ADDITIONAL INFORMATION FOR EACH CATEGORY OF PERSONAL DATA TO THE EXTENT THERE ARE DIFFERENCES]

The provision of the above information is required is required from you to enable us to perform our contract as managing agent. We will inform you at the point of collecting information from you, whether you are required to provide the information to us.

4. THE PERSONAL INFORMATION WE COLLECT AND USE: INFORMATION COLLECTED FROM OTHER SOURCES

We also obtain personal information from other sources as follows:

- [INSERT TYPE OF PERSONAL DATA] from [INSERT FULL DETAILS OF THE SOURCE]
- [INSERT ADDITIONAL INFORMATION FOR EACH CATEGORY OF PERSONAL DATA TO THE EXTENT THERE ARE DIFFERENCES]

5. HOW WE USE YOUR PERSONAL INFORMATION

We will typically collect and use this information for the following purposes:

- For the performance of a contract you have with our client and pursuant to which we are appointed as their agent.

  (and/or)

- For the purposes of our legitimate interests or those of a third party, but only if these are not overridden by your interests, rights or freedoms.

We seek to ensure that our information collection and processing is always proportionate. We will notify you of any material changes to information we collect or to the purposes for which we collect and process it.

6. WHO WE SHARE YOUR PERSONAL INFORMATION WITH

We routinely share the following categories of personal data:

- [BULLET POINT THE CATEGORIES OF PERSONAL DATA YOU, AS AGENT, ROUTINELY SHARE, E.G. NAME, ADDRESS, MOBILE TELEPHONE NUMBER ETC].

This personal information may be shared with the following categories of recipients:

- [INSERT CATEGORIES OF RECIPIENTS YOU MAY SHARE PERSONAL DATA WITH].

This data sharing enables us to perform our contract as managing agent.

[Some of those third party recipients may be based outside the European Economic Area — for further information including on how we safeguard your personal data when this occurs, see 'Transfer of your information out of the EEA'.]

We will share personal information with law enforcement or other authorities if required by applicable law.

We will not share your personal information with any other third party.

7. WHERE YOUR PERSONAL INFORMATION MAY BE HELD

Information may be held at our offices and those of our group companies, and third party agencies, service providers, representatives and agents as described above.

We have security measures in place to seek to ensure that there is appropriate security for information we hold including those measures detailed in our GDPR data protection policy.

8. HOW LONG YOUR PERSONAL INFORMATION WILL BE KEPT

- We will hold [INSERT CATEGORY OF PERSONAL DATA (EG NAME, ADDRESS AND CONTACT DETAILS)] for [INSERT PERIOD—[INSERT ADDITIONAL INFORMATION FOR EACH CATEGORY OF PERSONAL DATA TO THE EXTENT THERE ARE DIFFERENCES]

9. REASONS WE CAN COLLECT AND USE YOUR PERSONAL INFORMATION

We rely on [INSERT LAWFUL BASIS, E.G. CONTRACT] as the lawful basis on which we collect and use your personal data.

[NB, IF RELYING ON LEGITIMATE INTERESTS YOU WILL NEED TO INSERT WHAT THOSE LEGITIMATE INTERESTS ARE].

[INSERT DETAILS OF OTHER LAWFUL BASIS WHICH APPLY IN OTHER SITUATION / TO OTHER CATEGORIES OF PERSONAL INFORMATION AS APPROPRIATE.]

10. TRANSFER OF YOUR INFORMATION OUT OF THE EEA

[NB, ONLY ADD THIS SECTION IF YOU ARE TRANSFERRING DATA OUTSIDE OF THE EEA].

We may transfer your personal information to the following which are located outside the European Economic Area (EEA) as follows:

- [INSERT DETAILS ON FIRST COUNTRY/ TERRITORY] in order to [INSERT REASON FOR THE TRANSFER, EG TO PROVIDE YOUR NAME AND ADDRESS DETAILS SO THAT OUR OVERSEAS SUPPLIERS CAN SEND YOU THE GOODS YOU HAVE ORDERED]

- [INSERT DETAILS ON SECOND COUNTRY/ TERRITORY] in order to [INSERT REASON FOR THE TRANSFER]

Such countries do not have the same data protection laws as the United Kingdom and EEA. Whilst the European Commission has not given a formal decision that [SUCH COUNTRIES] provide an adequate level of data protection similar to those which apply in the United Kingdom and EEA, any transfer of your personal information will be subject to a [PROVIDE DETAILS OF THE APPROPRIATE OR SUITABLE RELEVANT SAFEGUARDS EG EUROPEAN COMMISSION APPROVED CONTRACT] (as permitted under [INSERT RELEVANT GDPR ARTICLE PERMITTING THE TRANSFER EG ARTICLE 46(5), WHICH THE ARTICLE 29 WORKING PARTY GUIDANCE CONFIRMS MUST BE SPECIFIED] of the General Data Protection Regulation that are designed to help safeguard your privacy rights and give you remedies in the unlikely event of a misuse of your personal information. To obtain a copy of the such [SAFEGUARDS] [INSERT DETAILS OF WHERE THEY HAVE BEEN MADE AVAILABLE (WHERE POSSIBLE PROVIDING A LINK TO THE MECHANISM OR INFORMATION.]

If you would like further information please contact [us OR [INSERT DETAILS], our Data Protection Officer (see 'How to contact us' below). We will not otherwise transfer your personal data outside of the [United Kingdom OR EEA] or to any organisation (or subordinate bodies) governed by public international law or which is set up under any agreement between two or more countries.

11. YOUR RIGHTS

Under the General Data Protection Regulation you have a number of important rights free of charge. In summary, those include rights to:

- fair processing of information and transparency over how we use your use personal information
- access to your personal information and to certain other supplementary information that this Privacy Notice is already designed to address
- require us to correct any mistakes in your information which we hold
- require the erasure of personal information concerning you in certain situations
- receive the personal information concerning you which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to a third party in certain situations
- object at any time to processing of personal information concerning you for direct marketing
- object to decisions being taken by automated means which produce legal effects concerning you or similarly significantly affect you
- object in certain other situations to our continued processing of your personal information
- otherwise restrict our processing of your personal information in certain circumstances
- claim compensation for damages caused by our breach of any data protection laws

For further information on each of those rights, including the circumstances in which they apply, see the Guidance from the UK Information Commissioner's Office (ICO) on individuals rights under the General Data Protection Regulation.

If you would like to exercise any of those rights, please:

- email, call or write to us OR [INSERT DETAILS]
- let us have enough information to identify you [(EG FULL NAME, ADDRESS AND PROPERTY ADDRESS)],
- let us have proof of your identity and address (a copy of your driving licence or passport and a recent utility or credit card bill), and
- let us know the information to which your request relates, including any account or reference numbers, if you have them

12. KEEPING YOUR PERSONAL INFORMATION SECURE

We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

13. HOW TO COMPLAIN

We hope that we can resolve any query or concern you raise about our use of your information.

The General Data Protection Regulation also gives you right to lodge a complaint with a supervisory authority, in particular in the European Union (or European Economic Area) state where you work, normally live or where any alleged infringement of data protection laws occurred. The supervisory authority in the UK is the Information Commissioner who may be contacted at https://ico.org.uk/concerns/ or telephone: [0303 123 1113].

14. CHANGES TO THIS PRIVACY NOTICE

This privacy notice was published on [INSERT DATE] and last updated on [INSERT DATE].

We may change this privacy notice from time to time, and when we do we will inform you.

15. [DO YOU NEED EXTRA HELP?

If you would like this notice in another format (for example: audio, large print, braille) please contact us (see 'How to contact us' above).]

APPENDIX IV

PRIVACY NOTICE GUIDANCE

GDPR: The New Data Protection Rules

Guidance relating to template privacy notice.

The General Data Protection Regulation (GDPR) which comes into force on 25 May 2018 requires all organisations to communicate privacy information to individuals (referred to as data subjects) whose personal data they are processing.

This privacy information is communicated in the form of a privacy notice.

You have received a template privacy notice. This document is a template in the truest sense of the word, and therefore you will need to populate the "blanks" as appropriate.

In practice, you are likely to have a suite standard privacy notices one for each category of data subject whose personal information you are processing.

You should bear in mind the following:

1. As part of the information audit, you will have considered what information you receive, and from what sources. Your privacy notice will need to specify types of data you are collecting. It is good practice to set out whether you are collecting this directly, or collecting from other sources.

2. There is no doubt that you are sharing data with external sources. This includes making data available for external sources too. Your privacy notice will need to set out the categories of those who you are sharing an individual's personal information with.

3. Your privacy notice will need to deal with retention of personal data. It may be that you have different retention periods for different types of data. Whatever your internal policy, you will need to set it out on your privacy notice. Your privacy notice may, therefore, set out that you intend to retain data whilst ever you manage the development and the data subject is a leaseholder, and that, once either they cease to be a leaseholder or you cease to manage the development, you keep the data for a specified number of years. You will of course need to specify the number of years that you intend to keep it for.

4. You will need to specify the lawful basis on which you collect and process the data.

5. If you are transferring information outside of the EEA, you will need to include the section in the privacy notice which deals with this.

6. The privacy notice sets out that you will keep personal information secure, and that you have appropriate security measures in place to prevent personal information being accidently lost, or used or accessed in an unauthorised way. You will of course need to ensure that you have such measures in place, and that your data protection policy deals with security.

7. You will need to ensure that you have appropriate internal policies and procedures so that you can demonstrate compliance.