

**Issued August 2018**

## **Briefing:**

# **General Data Protection Regulations (GDPR)**

### **Summary of key points:**

- The General Data Protection Regulations (GDPR), alongside the Data Protection Act 2018 (DPA), substantially strengthen previous law governing the storage and use of data. The DPA provides that GDPR, although an EU instrument, will continue to apply even after the UK leaves the EU.
- Data protection law now applies regardless of the format in which data is stored. The previous distinction between electronic and paper storage no longer applies.
- There are six grounds under which data may lawfully be processed. 'Contract' and 'legitimate interests' are likely to be the most important for housing associations.
- 'Consent' may also be helpful in some cases but housing associations should be cautious about using this ground because of the special requirements attached to it: in particular, it implies that the processing will not take place, or will cease, if the consent is withheld or withdrawn.

Contact name: John Bryant  
Job title: Policy Leader  
Direct line: 020 7067 1082  
Email: [john.bryant@housing.org.uk](mailto:john.bryant@housing.org.uk)

Lion Court  
25 Procter Street  
London WC1V 6NY

## 1. Background

---

As members will be aware, the new General Data Protection Regulations (GDPR) became law throughout the European Union on 25 May 2018. The law took effect on that date in the UK, as in all EU countries, without any requirement for legislation by national parliaments. The UK Government, however, brought forward a Data Protection Act, which operates in parallel with the GDPR and provides, among other things, that the GDPR will remain in effect within the UK even after 29 March 2019, the scheduled date for the UK to leave the EU.

In the UK, the agency with the primary responsibility for regulation and enforcement on data protection issues, including GDPR, is the Information Commissioner's Office or ICO.

The GDPR has received wide publicity and there is a substantial body of advice from the ICO and other reputable sources specialising in data issues. A selection of online resources will be found at the end of this briefing. It is not the intention of this briefing to duplicate this advice. The briefing does, however, draw out some aspects of data policy that will be of particular concern to housing associations either because of their role as social landlords or because of their regulatory status.

It should be made clear at the outset, however, that the GDPR does away with the former distinction between traditional paper storage of data and modern electronic formats. In general, data protection requirements will now apply to all formats in which data is held and used. A further point is the very broad meaning assigned to the word 'processing' in relation to data, which includes collection and storage as well as the actual manipulation and application of data. This briefing uses the word 'processing' in this broad sense.

GDPR Article 4 (Definitions): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

## 2. Lawful bases for data processing

---

This section sets out the six lawful bases for data processing and examines four of these in more detail, namely: contract, legitimate interests, vital interests and consent.

In practice, 'contract' and 'legitimate interests' are likely to be the most important. They both impose significant requirements on the data controller.

'Vital interests' is likely to be material only in very limited circumstances.

Contact name: John Bryant  
Job title: Policy Leader  
Direct line: 020 7067 1082  
Email: john.bryant@housing.org.uk

Lion Court  
25 Procter Street  
London WC1V 6NY

info@housing.org.uk  
www.housing.org.uk

'Consent', previously common as a basis for processing in the sector, is subject to important new restrictions that seriously limit its application (although it will remain useful in certain areas of work).

## The six lawful bases

Under GDPR, there are six grounds on which data may lawfully be processed. These are:

**(a) Consent:** the data subject has given clear consent for his or her data to be processed by the data controller for a specific purpose.

**(b) Contract:** the processing is necessary for a contract between the data subject and the data controller, or because the data subject has asked the data controller to take specific steps before entering into a contract.

**(c) Legal obligation:** the processing is necessary for the data controller to comply with the law (not including contractual obligations).

**(d) Vital interests:** the processing is necessary to protect someone's life.

**(e) Public task:** the processing is necessary for the data controller to perform a task in the public interest or for the data controller's official functions, and the task or function has a clear basis in law.

**(f) Legitimate interests:** the processing is necessary for the data controller's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data sufficient to override those legitimate interests.

[\(ICO online guidance: Lawful basis for processing\)](#)

## Contract

In the normal course of their business, housing associations routinely enter into contractual arrangements with a large range of individuals and organisations, including their employees, contractors and suppliers. This also includes, of course, their tenants and leaseholders (since every tenancy agreement and lease is legally a contract).

The GDPR has made very little difference to the processing of data for contractual purposes, which remains much as it was under the Data Protection Act 1998. Processing is permitted, not only to carry out obligations under the contract but also before the contract is entered into, if the data subject has agreed to the processing with a view to entering into the contract. Examples of this would include processing data in order to provide a business quote, or taking up employment references.

Much of the processing that housing associations do in relation to their tenants and employees will clearly be covered by this basis because the processing is evidently necessary if the association is to fulfil its obligations under a tenancy agreement or contract of employment.

Contact name: John Bryant  
Job title: Policy Leader  
Direct line: 020 7067 1082  
Email: john.bryant@housing.org.uk

Lion Court  
25 Procter Street  
London WC1V 6NY

However, this does not mean that all processing arising from the contract is necessarily covered.

For instance, a housing association may wish to process data to satisfy itself that the other party is complying with the terms of the contract. Processing for this purpose is not normally covered by the 'contract' basis because it is not necessary for the association to carry out its own obligations. It is, however, highly probable that processing for this purpose will be covered by some other lawful basis, notably 'legitimate interest' (see below).

### **Legitimate interests**

Where data is processed on the basis of 'legitimate interests', the following requirements apply.

- The data controller must be clear both with itself and with data subjects about the nature of those interests, and it must not use the data except in accordance with those interests.
- The data controller must consider whether the processing is 'necessary': i.e. could the controller's legitimate interests be achieved without processing the data? This test is subject to considerations of reasonableness, so that processing may still be regarded as 'necessary' if avoiding it would mean that the controller's legitimate interests could be achieved only in some unreasonably burdensome or laborious manner.
- The controller must also apply a 'balancing' test: that is, ensuring that the processing will not override the privacy rights of individuals.
- The controller should adopt safeguards designed to avoid the collection of data that is not required in furthering the controller's legitimate interests, and should also ensure that data is erased when it is no longer required. The collection of data for reasons of contingency will require care. It may well be reasonable to collect and retain data that will assist the landlord in preventing or detecting some future fraud, even if there is no reason at present to suspect fraud, but any such collection must be proportionate and based on a clear legitimate interest (i.e. preventing fraud). Housing associations should avoid collecting or holding data for vague or ill-defined reasons (e.g. 'it may come in useful one day.')
- The data subject does not have the right to require the data controller to cease the processing and/or erase the data (although such a right would exist if the data were being processed on the basis of consent).
- The data subject has the right to object to the processing, in which case the data controller must consider whether the objection overrides the controller's legitimate interests. This will depend on the circumstances. For instance, it might well be a legitimate interest of the association, as a social landlord, to process a tenant's data in support of an effort to find a solution (such as a transfer) to some housing issue that it believes is in the tenant's best interest. If, however, the tenant then objects to the processing on the grounds that he or she is not interested in this particular solution and will not accept it even if the landlord secures it, the landlord might then feel that it no longer has a legitimate interest in using the tenant's data for this purpose. But this is not,

Contact name: John Bryant  
Job title: Policy Leader  
Direct line: 020 7067 1082  
Email: john.bryant@housing.org.uk

Lion Court  
25 Procter Street  
London WC1V 6NY

of course, a blanket right for the tenant to block the use of his or her data. If the tenant were in serious breach of the tenancy, for instance, and the landlord had decided that possession action was necessary, the tenant would not be able to block processing for this purpose because the landlord's legitimate interests would take priority.

[See ICO guidance.](#)

### **Vital interests**

It has been suggested that certain types of processing may be justified on the ground of 'vital interests' where the processing is intended to protect the life of the data subject or some other person. Examples have been cited such as fire safety issues following the Hackitt review, and informing other agencies of vulnerable tenants who may need special assistance if there is a fire or other emergency.

However, housing associations are advised to use caution about basing processing on this ground. In the first place, it is intended for circumstances where a specific person's life is at immediate risk. It is not intended to cover more general risks that may crystallise at some point in the future, and it should not be seen as amounting to a general 'health and safety' ground.

Moreover, the ground is clear that if sensitive data is involved (as it would be, for instance, in the example of sharing details of vulnerable tenants), then consent should always be obtained unless the circumstances are so urgent that this is not possible.

It is suggested, therefore, that in most circumstances, except when an emergency has actually arisen, the 'vital interests' ground is unlikely to be useful to housing associations and other grounds, such as 'legitimate interests', and maybe in some instances 'consent', will normally be more relevant.

[See ICO guidance on 'vital interests'.](#)

### **Consent**

We are aware that many Federation members, sometimes on the basis of professional advice, have previously based their data processing largely or primarily on the consent of the data subject. In particular, some housing associations were advised to insert into their tenancy agreements a clause granting blanket consent by the tenant to the use of his or her data by the landlord for a wide range of purposes, or sometimes for any lawful purpose.

The Federation always had reservations about this approach. Such a sweeping consent meant that the tenant effectively forwent much of the protection he or she would otherwise have enjoyed under domestic or European data protection law, and the fact that the clause was incorporated into the tenancy agreement meant that it was virtually impossible to refuse.

While we do not question the legal advice received by members to the effect that that this form of consent was valid, we were concerned on policy grounds about asking tenants or housing applicants to give up their protection as a condition of tenancy, and it is for this reason that no such clause ever appeared in the Federation's model tenancies.

Contact name: John Bryant  
Job title: Policy Leader  
Direct line: 020 7067 1082  
Email: [john.bryant@housing.org.uk](mailto:john.bryant@housing.org.uk)

Lion Court  
25 Procter Street  
London WC1V 6NY

One of the most important changes brought in by GDPR is that consent may no longer be given on a blanket basis, nor may it be embedded in a wider agreement dealing with other issues. Where consent is sought, it must be in a manner that is specific about the proposed use, and nothing else may be contingent on whether the consent is granted or withheld.

Consequently, GDPR invalidates any clause in a tenancy agreement that purports to give consent for data processing, not only in new tenancies but also retrospectively in existing ones. In these circumstances, associations whose tenancy agreements contain such a clause are advised to remove it as soon as possible.

A further difficulty is that basing data processing on consent carries with it an acceptance on the part of the processing body that the data subject may withdraw his or her consent at any time and for any reason (or for no reason). In this event, the data controller must immediately cease to process the relevant data, and must delete them. According to the ICO, this applies even if the nature of the processing was such that some other lawful basis (such as 'legitimate interests') would have been available: in other words, once the data controller has committed itself to consent as a basis for processing, it cannot then rely on any other basis if the consent is refused or withdrawn. The withdrawal of consent, however, is not retrospective; it does not render unlawful any data processing undertaken when the data controller held valid consent.

In these circumstances we advise associations to consider very carefully to what extent they should use consent as a basis for processing data. If another lawful basis is available, such as contractual purposes or legitimate interest, it should certainly be used instead, meaning that the data subject's consent is not necessary. And where consent is not necessary, it should not be sought: associations should resist the temptation to make assurance doubly sure by seeking consent anyway ('just in case' the other lawful basis turns out not to be valid) because the seeking of consent carries with it an implication that the consent may be refused or withdrawn, in which case the relevant processing must cease.

The ICO advises:

"Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair."

Nevertheless, there may be some occasions where consent is the only lawful basis available, for example the supply to other agencies of personal information about vulnerable tenants. Consent in such cases should be sought explicitly (never by implication) in a manner that is not contingent on any other aspect of the relationship between the association and the data subject. The request for consent should specify exactly how and for what purpose the information will be used and whether and if so with whom it may be shared; and assurance should be given that it will be used only in the manner specified and will be deleted as soon as it is no longer needed. The request should also assure the subject that permission may be refused, or having been given may later be withdrawn, without prejudice to any other aspect of the data subject's relationship with the association.

Associations processing data on the basis of consent will need to set up mechanisms to ensure that they can promptly cease processing and delete the data if consent is withdrawn, and that these data will be removed as soon as the stated conditions of the consent, such as the

Contact name: John Bryant  
Job title: Policy Leader  
Direct line: 020 7067 1082  
Email: john.bryant@housing.org.uk

Lion Court  
25 Procter Street  
London WC1V 6NY

purpose for which it was given, cease to apply. Consent is, in short, a suitable lawful basis for processing only where the data controller is able to give genuine choice to the data subject and where the later withdrawal of the consent would not present operational challenges.

[See ICO guidance on consent.](#)

### 3. Individual rights under GDPR

---

This section looks at the rights of the individual under GDPR and in particular covers:

- the privacy notice
- the data subject's right of access to data
- the special requirements relating to direct marketing

#### Individual rights

The GDPR provides the following rights for individuals:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object
- rights in relation to automated decision making and profiling.

#### Notification of privacy information

Data controllers are required to provide privacy information to data subjects. Much of this is likely to be included in a 'privacy notice' but it may not always be sensible or practical to encompass all the necessary details in a single notice. Housing associations should consider taking a blended approach whereby the standard notice is supported by mechanisms such as brief notices that set out the key issues in which a data subject is likely to be most interested whilst signposting to fuller, more detailed sources such as the main privacy notice.

Contact name: John Bryant  
Job title: Policy Leader  
Direct line: 020 7067 1082  
Email: [john.bryant@housing.org.uk](mailto:john.bryant@housing.org.uk)

Lion Court  
25 Procter Street  
London WC1V 6NY

[info@housing.org.uk](mailto:info@housing.org.uk)  
[www.housing.org.uk](http://www.housing.org.uk)

It makes sense to provide privacy information through the same medium (e.g. online, on paper) as the data subject is using to engage with the housing association.

The privacy information that must be provided to the data subject is largely the same regardless of whether the data is being supplied personally by the data subject (or another individual (e.g. a parent or guardian if the subject of the data is a child)) or by a third party (see below for the points of difference). In all cases, therefore, regardless of the source of the personal data, the data subject (or other individual) must be informed of:

- the name of the organisation holding the data (i.e. the housing association), how to contact it, and (if it has one) its data protection officer
- the purpose for which the data is being processed (bearing in mind that 'processing' includes 'holding')
- the lawful basis for the processing
- where applicable, the 'legitimate interests' for the processing
- to which recipients or categories of recipient the data may be supplied
- details of any international transfer of the data
- details of any automated decision-taking, or profiling, for which the data will be used
- how long the data will be retained
- the legal rights of the data subject
- where consent is the lawful basis for processing the data, the right of the data subject to withdraw that consent
- the right to lodge a complaint with the ICO.

If the data is being sought from the data subject (or other individual), it is also necessary to indicate:

- whether the data subject (or other individual) is under a legal or contractual obligation to supply the data

If the data is obtained from a third party, the data subject must be advised of:

- the categories of personal data that have been obtained
- the source from which the data has been obtained.

Contact name: John Bryant  
Job title: Policy Leader  
Direct line: 020 7067 1082  
Email: [john.bryant@housing.org.uk](mailto:john.bryant@housing.org.uk)

Lion Court  
25 Procter Street  
London WC1V 6NY

The privacy information should be supplied at the time the data is obtained, if they are supplied by an individual. If the data comes from some other source, the data subject should receive the privacy information no later than the time at which the data is supplied to a third party or is used to contact the data subject or, in any case, within a 'reasonable time', which should not exceed one month.

Where the data is obtained from a third party, there are exceptions from the obligation to provide privacy information:

- if this would merely duplicate information already in the data subject's possession
- if providing the information would be impossible (e.g. if the housing association has no means of contacting the data subject) or would involve disproportionate effort
- if providing the information would thwart or seriously impair the purpose of processing the data
- if the housing association is legally obliged to obtain or disclose the data, or keep it secret.

The requirement to provide the privacy information does not necessarily mean that a physical privacy notice must be served providing the necessary details. This would be one way of doing it. Alternatively, it would be equally acceptable to include the information in a notice on the housing association's website, but in this case it should be easily accessible and the data subject should be made aware of it and advised how to find it (i.e. it would not be enough simply to place it on the website and assume the data subject will look for it).

Privacy information should be provided in clear, accessible language. Jargon and technicalities should be avoided.

### **Right of access**

There is a general (but not absolute) right of access, allowing data subjects to see what information is held about them. Such a request may be made verbally or in writing and the housing association, as data controller, is normally required to comply with it within one calendar month. The access should normally be provided free of charge: the previous provision allowing a fee of up to £10 no longer applies.

Associations may consider circumstances where the disclosure of information may compromise the association's legitimate purposes. An example might be where the association has accumulated a body of evidence suggesting, although not conclusively, that the property is no longer the tenant's only or principal home. In this situation, the association has a legitimate interest, if its suspicions are correct, in bringing the tenancy to an end so that the property can be let to someone in greater need of it.

In investigating the matter, the association might want to interview the tenant about his or her use of the property. This aim would be seriously compromised if the tenant, perhaps aware of the association's suspicions, were able to demand access to the association's files to ascertain exactly how much the association knows, and thus decide what must be admitted and what may plausibly be denied.

Contact name: John Bryant  
Job title: Policy Leader  
Direct line: 020 7067 1082  
Email: john.bryant@housing.org.uk

Lion Court  
25 Procter Street  
London WC1V 6NY

## **Data that may involve individuals other than the data subject**

It is in the nature of the data that housing associations are likely to hold about residents that often this data will involve identifiable individuals other than the data subject. In these circumstances the association must have regard to the interests of the other individual(s), and will need to consider very carefully whether, and if so how, to comply with the subject access requirement.

In some cases, it may be possible simply to supply the data with the other individual's name redacted. But often this will not be appropriate: for instance, the association's records concerning a tenant may include complaints received from neighbours or other residents about the tenant's behaviour, and it may well be obvious who made the complaint even if the name is blacked out. Associations should adopt a policy about circumstances in which data subject requests will not be complied with, in order to protect the interests of others. Any such policy, whilst clearly setting out the overall approach, should be flexible enough to allow each case to be treated on its individual merits.

This may incorporate, in some circumstances, a policy not merely of redacting information but of declining to confirm whether or not the requested information exists. For instance, a tenant might request details of complaints received from two specified neighbours. If the association has, in fact, received complaints from one of these neighbours but not the other, it would clearly be inadvisable to respond by saying that there is no record of a complaint by one of the specified neighbours, but that in respect of the other neighbour the information is redacted. The only way to prevent the obvious inference from being drawn is to adopt a clear policy that requests of this kind will not be complied with, even if the answer would have been that the information requested does not exist.

## **Excessive, unreasonable or vexatious requests**

Housing associations may occasionally receive a subject access request that involves data that is exceptionally bulky or particularly difficult to assemble. In such a case, the first step should be to go back to the data subject and seek to refine the request and identify more precisely the data required.

If, however, the request remains very broad, the association may consider that the effort involved is excessive or unreasonable. In this situation, the association may decide either to decline to comply with the request or to make a suitable charge reflecting the workload involved (although, in either case, the association should remain receptive to complying without charge to a more targeted request).

The Federation recommends that any failure to comply, or decision to charge, should be in accordance with a published policy and should be signed off at an appropriate level of seniority. It should be communicated to the data subject as soon as possible, and in any event within the one-month deadline for compliance, and the data subject should be advised how the decision may be queried or challenged and of his or her rights under data protection law to seek the advice of, or make a complaint to, the Information Commissioner's Office.

Contact name: John Bryant  
Job title: Policy Leader  
Direct line: 020 7067 1082  
Email: john.bryant@housing.org.uk

Lion Court  
25 Procter Street  
London WC1V 6NY

Similar comments apply if the association considers that access requests made by a data subject are vexatious by reason of their frequency, extent or content. Any refusal to comply on this ground should be notified to the data subject within one calendar month of the request and with details of how the decision may be challenged and the data subject's legal rights.

Associations should ensure that any decision not to comply with a request, or to charge for compliance, is justified as an exception to the normal rule of compliance. Such a decision should be based on the merits (or lack of merit) of the request itself, rather than on the association's perception of the data subject. (That is, even if a data subject has established a pattern of making unreasonable requests with which the association has decided not to comply, any further request from the same subject should be considered on its merits and complied with if possible. It should not automatically be ruled out simply because it comes from a subject that has made repeated unreasonable requests in the past.)

### **Importance of right of access**

This briefing reflects the fact that the nature of the sector means that there are likely to be occasions on which associations may consider, in accordance with their published policies, that data requested under the right of access may be refused altogether, or supplied only in a redacted form. However, this should not detract from the importance of the right of data access, and it is stressed that the default position, in response to a subject access request, should be to comply in full without redaction. Refusal to comply, or compliance only in part or subject to redaction, should be very much the exception and should occur only for clear and compelling reasons in accordance with an appropriate published policy.

### **Further rights**

There are a number of further rights that are not absolute, in the sense that the data controller need not comply with a request if there are clear reasons not to do so. The exact requirements vary according to the exact right being used, but they generally have in common that the data controller has one month either to comply or to explain why not. In general, housing associations should comply with requests when they reasonably can; any association minded not to comply should first consult the more detailed guidance on the ICO website.

These rights are:

- the right to request that inaccurate or incomplete data be rectified
- the right to request that data be erased
- the right to request that the data holder refrain from processing the data in certain ways
- a right to data portability
- a general right to object to the processing of data
- certain rights in relation to automatic decision-making and profiling.

Contact name: John Bryant  
Job title: Policy Leader  
Direct line: 020 7067 1082  
Email: john.bryant@housing.org.uk

Lion Court  
25 Procter Street  
London WC1V 6NY

## **Direct marketing**

There are specific requirements under GDPR in respect of 'direct marketing'.

In particular, there is a blanket right for the data subject to object to direct marketing, in which case it would be an offence to continue to market directly to this individual.

Concern has been expressed by some associations because newsletters and other routine communications with residents may sometimes include an element of advertising of good or services available from the housing association or from third parties (for instance, if the association agreed to include in its newsletter a notice about a forthcoming local fete).

The ICO has confirmed that advertising counts as 'direct marketing' only if it is specifically directed to the individual recipient. Thus, an advertisement targeted at a specific recipient is 'direct marketing' (to which there is a right to object), whereas more general advertising is not.

It should also be noted that the Privacy and Electronic Communications Regulations (PECR) remain in force and although beyond the scope of this briefing they should be consulted before embarking on any electronic marketing activity.

See [ICO guidance on direct marketing](#) and the [Privacy and Electronic Communications Regulations \(Statutory Instrument 2003/2426\)](#).

## **4. Regulatory and operational issues**

---

This section picks up a range of operational and regulatory issues:

- the approach of the Information Commissioner's Office to its regulatory role
- how duties under GDPR and the Data Protection Act relate to the Regulatory Framework, in particular to the requirement to comply with 'all relevant law'.
- the Data Protection Impact Assessment
- the role of the data protection officer

### **GDPR compliance**

Existing data protection law is already complex and demanding, and will be more so after GDPR takes effect. For an organisation to state definitively that it is 100% compliant is probably impossible. The ICO has made it clear that it will exercise its regulatory function in a proportionate and reasonable manner, and that its more stringent enforcement powers, including the swingeing fines provided for in GDPR, are likely to be used only for unusually gross or flagrant breaches.

Contact name: John Bryant  
Job title: Policy Leader  
Direct line: 020 7067 1082  
Email: [john.bryant@housing.org.uk](mailto:john.bryant@housing.org.uk)

Lion Court  
25 Procter Street  
London WC1V 6NY

What is important is that organisations should be aware of their responsibilities and should be able to show that they are taking all reasonable steps to comply with them. Housing associations should therefore take a proportionate approach to data protection, seeing it as something that can be enabling for a business and not necessarily a burden.

Any data breach, or other failure to comply with GDPR, the Data Protection Act or the association's own procedures, should be recorded and reported at an appropriate level of seniority. Serious breaches should be reported to the ICO and RSH.

### **Compliance with regulatory standards**

Some members have expressed a concern that the Regulatory Framework may require them to alert the Regulator of Social Housing (RSH) if they were not fully in compliance with GDPR immediately after it became a legal requirement on 25 May 2018.

Paragraph 1.1 of the Governance and Financial Viability Standard states that providers' governance arrangements must (among other things) ensure 'compliance with all relevant law'. The associated Code of Practice says, in paragraph 19, the providers must advise the RSH 'at the earliest opportunity about any material issues that indicate there has been or may be a breach of the standards'. Paragraph 19 goes on to cite the following as examples of what might constitute a 'material' issue: 'material frauds, liquidity issues, breaches of lenders' covenants or failures of governance'.

It is relevant here to consider the approach taken to the GDPR by the Information Commissioner's Office (ICO), which is the principal UK regulator concerned with enforcing the GDPR. The ICO has acknowledged that many entities, in all parts of the economy, were not fully compliant on 25 May 2018 and that absent any special aggravating circumstance it does not intend to exercise its enforcement powers in a rigorous or heavy-handed way provided that organisations are aware of their obligations under GDPR and are working towards full compliance within a reasonable period of time.

The Federation has raised this question with the RSH, which has indicated that if a provider is compliant with previous data protection law and is working towards full compliance with the new requirements of GDPR, it would be reasonable for the provider to regard failure to achieve full compliance by 25 May as not presenting a 'material' issue for the purposes of paragraph 19 of the Code of Practice. Obviously, though, prompt and timely notification will be required if a data protection issue arises that presents a higher degree of 'materiality' comparable with the examples given in paragraph 19.

### **Data Protection Impact Assessment**

A Data Protection Impact Assessment (DPIA) is a tool enabling the data controller to identify, manage and minimise involved in any exercise that involves data processing. A DPIA must be carried out if the data is likely to give rise to a high risk for individuals. Clearly, most of the work of associations involves the use of highly sensitive personal data pertaining to tenants or other individuals so a DPIA will be needed. It is not mandatory in other cases, although associations may find a DPIA useful for major projects generally.

Contact name: John Bryant  
Job title: Policy Leader  
Direct line: 020 7067 1082  
Email: john.bryant@housing.org.uk

Lion Court  
25 Procter Street  
London WC1V 6NY

A DPIA must:

- describe the nature, scope, context and purposes of the processing
- assess necessity, proportionality and compliance measures
- identify and assess risks to individuals
- identify any additional measures to mitigate those risks.

The assessment of risk should consider both the severity of harm, if it occurs, and the likelihood that it will occur. If the DPIA discloses a high risk that cannot be mitigated, the association should inform the ICO before commencing the processing. The ICO will provide written advice within eight weeks (fourteen weeks in complex cases) and may choose to warn against or prohibit the proposed processing.

[See ICO advice on DPIAs.](#)

### **Data protection officer**

Because housing associations are not public bodies, they are not formally required to appoint a data protection officer (DPO). Nevertheless, it is considered advisable when an organisation processes a significant amount of sensitive data.

It is very likely that housing associations are likely to fall into this category, given their role as social landlords dealing with many vulnerable individuals and groups.

There is no expectation that the DPO must be a dedicated position; on the contrary, the role will normally be assigned to an existing officer or employee. However, the DPO should be provided with training about the role and the function may well, depending on the size of the association and the nature of its work, demand a significant time input. Associations will have to consider carefully how and by whom the DPO function will be discharged.

Designating the chief executive as DPO, for instance, is likely to result in most organizations in the delegation of most of the day-to-day function to someone else. In this case, it may be better to designate that person as DPO, rather than the chief executive, to avoid doubt about where the responsibility lies. Some organisations have found it works well to designate their IT manager as DPO, while others have avoided this because of the conflict of interest if it is the actions of the IT department that raise questions for the consideration of the DPO. The designation of an appropriate DPO is, therefore, a matter for each organisation to determine, but it is likely to be someone with a general understanding of the organisation's practices and requirements in terms of using data, and of a sufficient level of seniority to have authority in internal discussions.

### **Procurement**

The nature of housing associations' business means that they are likely to have several procurement contracts for goods and services, e.g. repairs, disabled adaptations, money advice. As data controllers they have overall responsibility for ensuring that contractors are delivering these services and managing customers' personal data (sometimes sensitive) on the association's behalf safely and effectively. Associations should ensure that management of data

Contact name: John Bryant  
Job title: Policy Leader  
Direct line: 020 7067 1082  
Email: [john.bryant@housing.org.uk](mailto:john.bryant@housing.org.uk)

Lion Court  
25 Procter Street  
London WC1V 6NY

features in all contracts from the very beginning of the procurement process and throughout the term of the contract.

### **Document retention and disposal**

With the support of a number of members, whose assistance is gratefully acknowledged, the Federation has updated version of its guidance to members on the retention and disposal of documents.

## **5. Conclusion**

---

The GDPR and the Data Protection Act 2018, taken together, represent a major evolution in data protection law within the EU generally and the UK in particular. Over time, as the new law beds in, practical issues will emerge to be considered by the ICO and the domestic and European courts. Moreover, information technology itself will advance as devices and programmes are developed and improved. In these circumstances, recognised good practice is likely to evolve, possibly quite rapidly, and associations will need to keep abreast of developments.

A number of Federation members have contributed substantially to the development of the guidance. We are pleased to acknowledge their support and advice. Responsibility for any errors or oversights, of course, remains with the Federation.

This briefing represents the Federation's position as of October 2018.

Federation contacts:

**John Bryant**

Policy Leader

[john.bryant@housing.org.uk](mailto:john.bryant@housing.org.uk)

020 7067 1082

**Paul Bayly**

Governance and Compliance Manager

[paul.bayly@housing.org.uk](mailto:paul.bayly@housing.org.uk)

020 7067 1036

Contact name: John Bryant  
Job title: Policy Leader  
Direct line: 020 7067 1082  
Email: [john.bryant@housing.org.uk](mailto:john.bryant@housing.org.uk)

Lion Court  
25 Procter Street  
London WC1V 6NY

[info@housing.org.uk](mailto:info@housing.org.uk)  
[www.housing.org.uk](http://www.housing.org.uk)