September 2018

APSCO GDPR FAQS 2018 V4

These FAQs incorporate and replace V1, V2 and V3.

These FAQs are for guidance only and are not legal advice. They have been prepared by APSCo's General Counsel. You should instruct your own GDPR expert lawyer for bespoke legal advice and details of our Legal Affiliates are on our website.

The GDPR is a highly complex legal document. Our FAQs are intended to be easy to read and give guidance to recruiters on specific concerns. Therefore, the information is simplified and may not be sufficient for your needs. Commentary on issues specific to recruitment is partially based on opinion, in light of the writer's knowledge of GDPR and the recruitment industry's response to it at time of writing.

These FAQ's will be updated periodically.

The ICO have prepared an overview which you can see here: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/.

The ICO have also prepared a series of Data Protection Self-Assessment Toolkits which can be a helpful steer for you on priorities: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment-toolkit/.

Please note these FAQs give information on how the GDPR is applicable in the UK. The GDPR is interpreted differently in other member states and there may be a stricter interpretation e.g. when explicit consent must be obtained. You should take your own legal advice if you control and process data in other EU countries.

Who does the GDPR apply to?

The GDPR applies to 'controllers' **and** 'processors' of personal data. The controller decides why and how personal data is processed and the processor acts on the controller's instructions.

Every organisation or sole trader who processes personal information have to pay a data protection fee to the ICO, unless they are exempt. On the ICO website there is a test to see whether you are exempt or if you need to register and thereby pay the fee: https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You have significantly more legal liability if you are responsible for a breach than under the previous Data Protection Act 1998 (DPA 1998).

As a controller, you are not relieved of your obligations where a processor is involved – the GDPR requires you to enter specific terms with your processors to comply with the GDPR.

The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

The GDPR does not apply to certain activities including processing for national security purposes (which is covered by the Data Protection Act 2018) and processing carried out by individuals purely for personal/household activities.

What are the basic tenets of the GDPR?

The GDPR sets out rules for collecting and processing personal information, which is information identifying and relating to an individual.

Companies processing personal data are required to abide by article 8 of the GDPR, which requires that data must be:

- Fairly and lawfully processed.
- Processed for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to the processing purposes.
- Accurate.
- Kept for no longer than necessary.
- Processed in a manner that ensures appropriate security of the personal data.

The definition of "processed" is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes both hard and soft copy data.

What is personal data?

'Personal data' is any data that identifies a living individual and relates to that individual. The GDPR's definition is more detailed than previous data protection legislation and make it clear that information such as an online identifier e.g. an IP address, location trackers and ID numbers is personal data.

The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria e.g. chronologically ordered manual data. So, it is unlikely to cover personal data left on people's desks and drawers BUT there are general confidentiality issues and data security issues arising from poor management of data.

Do we need to register with the Information Commissioners Office (ICO)?

Yes, an organisation that controls and processes data should register with the Information Commissioners Office. https://ico.org.uk/for-organisations/register/.

The Data Protection Act 2018 requires every data controller (eg organisation, sole trader) to register with the ICO, unless they are exempt.

The cost of your data protection registration depends on your size and turnover but for most businesses it costs £35. The payment is always VAT: nil

You'll only need to pay £500 if you have:

- a turnover of £25.9M **and** more than 249 members of staff; or
- if you are a public authority with more than 249 members of staff.

As a recruiter are we a controller or a processor? We are receiving data processing agreements from our clients.

You will be a controller when carrying out most of your activities. If your clients send data processing agreements you should push back and ask what personal data they think you are processing on their behalf and the nature of the processing, as you consider you are a data controller. They need to provide this and other information for the agreement to be binding. You could compromise by signing but the schedule stating that you will only process data if and when notified by them.

If you are an MSP, you may be processing client data and hence a data processing agreement is required.

What is special category personal data?

Special categories of personal data is sometimes referred to as 'sensitive personal data'. Sensitive personal data means personal data consisting of the following in relation to the individual;

- Racial or ethnic origin.
- Political opinions.
- Religious (or other similar) beliefs.
- Membership of a trades union.
- Physical or mental health condition.
- Sex life and sexual orientation.
- Commission or alleged commission of any offence (Data Protection Act 2018).
- Any proceedings for any offence or alleged offence, or any information relating to the disposal or outcome of the proceedings (Data Protection Act 2018).

Is collecting passport and DBS information considered sensitive personal data?

Potentially by collecting a scan of a passport you are collecting special category data if it reviews race for example. Consent is not the only lawful processing ground for special category data. Legal obligation may be a lawful reason to collect a scan of a passport if it is to comply with legal right to work.

Can we still ask questions about candidates' or contractors' health?

Because of data protection laws you should only collect 'necessary' information. Furthermore the NUT (The National Union of Teachers) takes the view that the practice of issuing pre-employment health questionnaires to all job applicants, rather than to the successful job applicant(s), is likely to be unlawful given the general prohibition in the Equality Act against pre-employment health enquiries.

If you ask all candidates for the same information in, e.g. an application form you will have a great amount of sensitive data that is:

- possibly unnecessary (for example in case the candidate does not advance);
- potentially irrelevant (for example if perfect eyesight is not necessary for the role, don't ask); and
- could give grounds for discrimination claims.

Therefore, for roles that don't require information about the candidate's or contractor's health, it is better to simply not collect the data. For roles where health data is required (for example, for working with children or on a construction site), it is advisable to wait as long as possible to ask for health data. By waiting you only have to ask the candidate who has been invited for a second or final interview (or preferably, who has been offered the job) for health data specifically relevant for the role. This way, you can limit the data that is in fact 'necessary' to collect, seeing as you would only ask for health data relating to the role in question. You are also facing a smaller risk of discrimination claims, since you are giving all candidates the largest opportunity possible to being offered the job. However, you will always need to bear timing in mind and the importance of having the information if the candidate is appointed.

When does a Data Protection Officer have to be appointed under the GDPR?

You must appoint a data protection officer (DPO) if you:

- are a public authority (except for courts acting in their judicial capacity);
- carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

You may appoint a single DPO to act for a group of companies or for a group of public authorities, taking into account their structure and size.

Any organisation is able to appoint a DPO. Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations under the GDPR.

Whether you need to appoint a DPO depends on your business and you may need independent advice. However, those that process special categories of data or criminal convictions e.g. those recruiting for social work, education or banking as their core activity and on a large scale, will do. Your core activities are the

primary business activities of your organisation. So, if you need to process personal data to achieve your key objectives, this is a core activity.

Given the importance of personal data to recruitment operations you can appoint a DPO if you wish, even if you aren't required to. If you decide to voluntarily appoint a DPO, you should be aware that the same requirements of the position and tasks apply had the appointment been mandatory.

You may therefore decide to appoint a sole point of contact at a senior level or a small team with responsibility for data protection. If you decide that you don't need to appoint a DPO, either voluntarily or because you don't meet the criteria, the ICO suggest it would still be a good idea to record this decision to help demonstrate compliance with the accountability principle.

You must make your own decision on whether you have to have a DPO based on your own business operations and taking your own legal advice if necessary.

See the guidance on appointing a DPO here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

What is the specification of a statutory DPO role?

The statutory DPO's minimum tasks are to inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws, to monitor compliance, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits and to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

They must report to your board, operate independently and not be dismissed or penalised for carrying out their DPO duties and must have adequate resources to be able to meet their obligations. Their other duties, if any, must be compatible with their duties as a DPO. You can, as an alternative, appoint a DPO external to your organisation, which may be a sensible option for the largest multi-national groups or indeed for smaller businesses that nonetheless conclude they need or want a statutory DPO.

The GDPR is not specific about qualifications but a DPO should have professional experience and knowledge of data protection law. This should be proportionate to the type of processing your organisation carries out, taking into consideration the level of protection the personal data requires. Even if you decide you don't need a statutory DPO it is sensible to use this specification as a guide.

How can I process data compliantly?

In simple terms you have to comply with the principles of fair in Article 5, summarised below:

- Be transparent in relation to the data subject.
- Tell the data subject what you are collecting the data for – be specific about what your purposes for processing data are.

- Only collect what you need for the stated, legitimate purposes.
- Keep the personal data up to date and accurate – inaccurate data must be deleted or rectified.
- Don't keep data in a form that allows identification of the data subject for longer than necessary for the legitimate purposes notified to the data subject.
- Keep the data secure.

Keep these principles in mind as you work with personal data to keep your business compliant. You are held accountable to the data subjects and must document and show how you comply with these principles.

Furthermore, in regard to the internal process:

- Understand your data: what you collect and hold, where you store it, why you need it, what you do with it and how long you keep it for.
- Make sure that data protection policies and procedures are up to date – including privacy policies, data collection forms and internal data protection and retention policies.
- Check the basis on which you control and process personal data e.g. consent, legitimate interest, contractual obligation, legal obligation, public interest or vital interest.
- Ensure marketing-team practices are compliant with the GDPR, the DPA and marketing regulations - via appropriate use of databases, opt-ins, or 'recommend a candidate' and headhunting schemes.
- Ensure all arrangements with third parties who process data on your behalf are in writing and contain the legally required data protection clauses.
- Consider who may be your co-controllers – this could include MSP providers.
- Review your ICO notification to ensure it is accurate and up to date. Failure to notify new processing activities within 28 days is a criminal offence.
- Have robust subject access request procedures – failure to comply with these requests (e.g. by disgruntled job applicants) is the main reason for ICO complaints.
- Have a data security and security breach policy in place and communicate it to your employees.
- Educate your staff in data protection procedures; how you are processing data, for what reasons and on what grounds. For example, when it comes to retention, the GDPR can be seen as conflicting in regard to the Conduct Regulation.

What is a Privacy Notice?

A privacy notice informs data subjects about how an organisation collects, uses, stores, transfers and secures personal data. The GDPR defines personal data as "any information relating to a data subject" i.e. an individual.

Under Article 13 of the GDPR a party is required to provide an individual with certain information when their personal data (PD) is collected. The information that needs to be provided to data subjects is set out in this privacy notice template.

The ICO has issued guidance on privacy notices: transparency and control which has been updated to refer to the GDPR (www.ico.org.uk).

What do we need to include in our Privacy Notice?

Under Article 13 of the GDPR a party is required to provide an individual with certain information when their personal data (PD) is collected.

- The identity and contact details of the controller;
- Contact details of the data protection officer where applicable or the person responsible for data compliance in your business;
- Purposes of the processing and the legal grounds for processing and if based on legitimate interests what these are;
- The recipients of the personal data;
- Where applicable, if you intend to transfer personal data to a third country outside of the EU;
- The period for which the data will be stored or if not possible then the criteria to determine the period;
- The existence of the rights to request a subject access request, right to rectify data, right to delete data, right to restrict processing and right to data portability;
- Where process is based on consent, the right to withdraw consent at any time;
- The right to lodge a complaint with the ICO; and
- The existence if any of automated processing or profiling.

The ICO has issued guidance on privacy notices: transparency and control which has been updated to refer to the GDPR (privacy notices, transparency and control). You can find our privacy notice template and guidance here.

The ICO has issued a checklist which you can follow once you have completed your data audit and data mapping: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/.

Should a Privacy Notice be provided if the personal data is sourced from a third party?

Article 14 sets out the information to be provided where the data has not been obtained from the data subject e.g. from a job board or LinkedIn. In addition to the information to be provided as set out in the privacy notice the following information must be provided:

- The categories of personal data collected
- The source of the personal data and, if applicable, whether it came from publicly accessible sources.

Additionally, the party giving the data to you may need to disclose to the data subject the fact they are disclosing their data to you.

This information needs to be specific and cannot be provided in the form of generic information. A process is needed to ensure this information is provided to the individual in a separate notification within a reasonable period after obtaining the data but latest within a month. The information must be provided at latest at the

time of the first communication with them or prior to disclosure to a third party, even if that is less than a month.

There is an exception to Article 14 on the grounds that the provision of such information proves impossible or would involve a disproportionate effort. In such cases, it may be sufficient for the controller to protect the data subject's rights and legitimate interests, inter alia by making the information publicly available e.g. privacy notice on their website. This could potentially apply to **headhunting,** although headhunting must be considered very carefully and bespoke advice taken as there is a risk of non-compliance. The exception in Article 14 is applicable particularly when it comes to processing in the public interest or for scientific, historical or statistical research, not necessarily for commercial interests.

Organisations doing business in multiple jurisdictions face compliance challenges. They need to choose between a single global privacy notice and jurisdiction specific notices. Even within the EU member states have varying rules.

What is the difference between a privacy notice and a privacy policy?

Because of misunderstandings from many parties, the privacy policy and privacy notice are often seen as synonyms, which however, is not the case. A **privacy policy** is similar to your data protection policy. It is an internal policy, made for your employees as a procedural code. It explains how an organisation controls and processes data and how the business shall comply with its record keeping obligations under Article 30, if applicable. A **privacy notice** is an external document and explains to the data subject why you need their data, how you'll process it, how long you need it for and the individual's rights and is based on the privacy policy. There may be some overlap in content between the two.

Neither document is legally required but they are efficient tools to fulfil legal requirements and inform your employees and inform the data subjects. Without the policy and the notice, you would constantly have to personalise the flow of information to the other parties: 1) every employee would have to be separately educated in data protection (since there would be no handbook with policies) and 2) you would have to tick off all points of information in Article 13 GDPR whenever you collected data from a data subject, instead of giving the individual a concluded and pre-completed notice.

What are the lawful grounds for processing personal data?

It is important that you determine your lawful basis for processing personal data and document this, because your processing of data has an effect on individuals' rights. For example, if you rely on someone's consent to process their data, their right to revoke their consent and have the data deleted, is generally stronger than your reasons for the data to be retained.

There are four lawful grounds particularly relevant to recruiters:

- Explicit consent. Implied consent will no longer be adequate.
- The processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract to which the data subject is party.

- The processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject (for example, to provide work-finding services).
- Processing is necessary for compliance with a legal obligation to which you are subject (for example, keeping accountancy records).

There are also the legal basis of vital interest and processing because of public interest. Public interest however, only applies when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Vital interest, it has been said, will mainly apply in situations of life-or-death.

Can I only rely on one ground per data subject?

No, you can rely on different grounds for different uses. The ICO is not prescriptive about when each ground should be used however.

Which grounds you rely on for which activities will depend on the data you hold, how you use it and the nature of your recruitment business.

It will also depend on your approach to GDPR – you may choose to rely on legitimate interest for holding data on your database (as long as you have considered the balancing test properly (see below)), whilst another recruiter may decide that they will only hold data for which they have explicit consent to undertake specified activities. A blanket explicit consent is not enforceable.

If you have one database across your operations in different countries then a more consent based approach may be advisable to comply with stricter standards in other countries e.g. Germany and the Netherlands. You then need to ensure that the wording used is either country specific or sufficient across multi-jurisdictions.

Whatever approach you take to be compliant with the GDPR, you must abide by the fundamentals of data protection: the data subject must know what data you hold and what you do with it; the data should be accurate, not kept for longer than necessary and must be securely kept.

Do we need to obtain explicit consent from candidates to keep them on our database?

You will only need to do this if you have chosen consent as your basis for processing; it will depend on your approach to the GDPR. You may choose to rely on legitimate interest for holding data on your database (as long as you have considered the balancing test properly (see below)), whilst another recruiter may decide that they will only hold data for which they have explicit consent to undertake specified activities.

If you have set a specific retention period in your retention policy and that time period is up, we would recommend you to ask if the individual in question still wants to be on the database. This in order to not retain the data for 'longer than is necessary'. However, this is mainly if you have not been using the data. If

you for example, are actively using a temporary worker that has been on your database for the set retention period, it can be assumed that the worker would like to remain on the database.

It's already a legal requirement when making an introduction of an identifiable CV to a client to obtain consent from the candidate under The Conduct of Employment Agencies and Employment Businesses Regulations (Conduct Regulations). However, in the act of finding a suitable role for which to introduce the candidate you could be relying on your legitimate interest, as that is the service you provide. See below information on legitimate interest. Once a contract is anticipated or is entered into then the contract ground is appropriate.

If you have a statutory obligation to retain data for a certain period, you are relying on legal obligation and again under the Conduct Regulations, there is a duty to retain records for at least a year after their creation and at a least one year after the date on which you last provided work-finding services.

You should always consider whether you are being sufficiently transparent and whether the data subject would expect the particular use of their data.

The Privacy and Electronic Communications Regulations (PECR) relates to how people send electronic communications to their customers. There are some very important points in here for recruiters. The GDPR focuses more on how the data is collected, stored and used on an ongoing basis.

Under the PECR you need consent to market to individuals (including Ltd company workers), unless you have marketed them about similar services to those you've performed for them previously. It is expected that PECR will also be updated and that GDPR consent will be required. However, the ICO states that you can rely on legitimate interests for marketing activities if you can show that how you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object – but only if you don't need consent under PECR. Therefore the question of what is marketing in the context of your communications with your candidates and contractors will be very important.

How can we contact/market to prospect clients whilst still being compliant?

Client data is personal data. Even an individual's business email address can be considered personal data as GDPR defines 'personal data' as any information which may be attributed to an identified, or identifiable, individual and relates to that individual. This also means that data relating to an IP address, personal identification number, or account identification number is personal data in exactly the same way as information relating to a name, identity, or physical address. Client data will be a much lower risk processing than candidate data however, you should still be careful of the information you are recording on specific individuals.

If these are existing clients, **Recital 47** indicates that legitimate interests is likely to apply where you have a 'relevant and appropriate relationship', for example, because they are your client or employee. If you don't have a pre-existing relationship, it is harder to demonstrate that the processing can be reasonably expected. If you obtained the data from a third party, you need to be clear what the individual was told about when that data might be passed on for use by others, and whether this covers you and your purpose for

processing, as this will affect reasonable expectations. You will likely cover this by always providing a clear privacy notice.

According to the ICO the below is allowed for B2B marketing. This however, needs to be balanced with the rules in the GDPR:

Live Calls	▪ Screen against the Corporate Telephone Preference Service (CTPS). ▪ Can opt out.
Recorded calls	▪ Consumer must have given caller specific consent to make recorded marketing calls.
Emails or texts	▪ Can email or text corporate bodies. ▪ Good practice to offer opt-out. ▪ Individual employees can opt out.
Faxes	▪ Screen against the Fax Preference Service (FPS). ▪ Can opt out.
Mail	▪ Can mail corporate bodies. ▪ Individual employees can opt out.

To conclude:

- Candidate/Ltd company/Self-employed: treat as personal data but you can market relevant services, but provide an opt-out.
- Personal business data (e.g. an individual's email address): personal data but you can market relevant services, but provide an opt-out.
- Generic business data (e.g. an email address like info@ or accounts@): you can market, good practice to offer opt-out.

What are the PECR and what do they cover?

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) provide rules about sending marketing and advertising by electronic means, such as by telephone, fax, email, text and picture or video message, or by using an automated calling system. PECR also include other rules relating to cookies, telephone directories, traffic data, location data and security breaches.

What is considered marketing?

A definition of direct marketing is contained within the Data Protection Act 2018: Direct marketing means the communication (by whatever means) of advertising or marketing material which is directed to particular individuals. Direct marketing covers the promotion of aims and ideals as well as the sale of products and services.

Can we send marketing e-mails to clients and candidates on our data base or do we have to prove that they have explicitly consented/ 'opted in'?

Pre-ticked boxes do not comply with the explicit consent requirements of the GDPR. People must opt-in to your marketing activities, rather than opting out. Unsolicited marketing is, to a certain extent, still allowed for example over the phone. However, PECR include further rules on marketing than the GDPR. The ICO has produced a pedagogical Marketing Checklist for more guidance, which is in our GDPR toolkit.

Is sending a job spec to multiple candidates considered marketing and therefore something we have to have consent for?

There is a point when sending a job specification to multiple candidates ceases to be providing a service and is in reality a marketing email to try to raise interest in your services.

Any email must be targeted to that candidate so it's really important that you code candidates as accurately as possible on your system.

If an email is in effect marketing, there should be an opt-out (e.g. via mailchimp and similar providers). Your system then needs to set anyone who clicks the opt-out to "no marketing". You should be as particular in terms of managing their preferences as you can be. Self-service is ideal to encourage candidates to keep their data up to date and tell you what communication they want to receive. You should consider linking to your privacy notice in every candidate communication too.

Can I send unsolicited marketing emails without consent?

You should not send marketing emails or texts to individuals without specific consent. There is a limited exception for your own previous customers, often called the 'soft opt-in'. The term 'soft opt-in' is sometimes used to describe the rule about existing customers or in recruitment terms existing candidates and or clients. The idea is that if an individual gave you their details, and did not opt out of marketing messages, they are probably happy to receive marketing from you about similar products or services even if they haven't specifically consented. However, you must have given them a clear chance to opt out – both when you first collected their details and in every message you send. The soft opt-in rule means you may be able to email or text your own clients and candidates, but it does not apply to new contacts.

How can we collect consent and when do we have to have consent?

Consent must be a clear affirmative act, specific and informed indication of agreement to process personal data relating to the individual. This means you should be clear about the different uses you may make of the data.

Although consent can be collected by other means e.g. email or even a phone call, a tick-box consent is highly recommended. The consent must be clear, specific and detailed.

You must obtain explicit consent for automated decision-making, including profiling, which produces legal effects on the Data Subject. Generally recruitment decision making involves an element of human decision making but you should consider your own business.

You may rely on explicit consent to process special personal data although other grounds are set out in Article 9, GDPR.

Can we use legitimate interest for our processing so we don't need to have consent from everyone?

Processing is lawful if it is necessary for the purposes of the legitimate interest pursued by the controller (you) or a third party except where protecting the interests and rights of the data subject are more important, particularly if the data subject is under 18.

To make this decision you need to do a "balancing test".

Legitimate interests is the most flexible lawful basis for processing and probably the most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. It is our opinion that legitimate interest is suitable for most of your processing as a recruitment company.

The GDPR does not define what factors to take into account when deciding if your purpose is a legitimate interest. It could be as simple as it being legitimate to start up a new business activity or to grow your business. Therefore, you would imagine that an individual who has applied directly for a role or has advertised their role on a job board would reasonably expect processing of their data.

If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.

There are three elements to the legitimate interest's basis. It helps to think of this as a three-part test. You need to consider:

- Purpose test: are you pursuing a legitimate interest?
- Necessity test: is the processing necessary for that purpose?
- Balancing test: do the individual's interests override the legitimate interest?

The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.
The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.

You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.
You need to document your decisions on legitimate interests so that you can demonstrate compliance under the GDPR accountability principle. You must also include information about your use of legitimate interest

and your purposes for processing in your privacy notice. See more information about your privacy notice in the toolkit.

If you have decided to use legitimate interests as your lawful basis please review the ICO guidance thoroughly: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

When would we use the "contract" ground?

Processing is lawful if the personal data is necessary for the performance of a contract to which the data subject is a party or to take steps prior to entering into a contract. For example, if a candidate sends you their CV in response to a job advert they have sent it to you as they want to enter into a contract of employment with the client. Therefore the "contract" ground can be used in the context of this introduction. However, what if you want to send their CV to another client?

This is a harder condition to rely on as you will probably use the data for broader purposes and therefore will need explicit consent to process for other purposes, such as sending their CV to another client. You may choose to rely on the legitimate interests ground to hold their data on your database generally.

Can we download CVs from job boards?

The job boards have to make sure that their service of storing CVs and providing them to recruiters is GDPR compliant. It is your responsibility to make sure that you only work with job boards that are GDPR compliant (third-party due diligence) by for example reviewing the job boards' privacy terms for candidates. It is up to the job board what legal ground they are relying on for data processing, but most job boards are probably relying on consent. The candidate would in other words give their explicit permission for their CV to be on the job board – it is likely that they will have options about how broadly their data is used by the job board and by the job board's clients (e.g. signed up recruiters). A candidate may give explicit consent for their CV to be downloaded by anyone or expect to be asked before download. This consent does not extend to recruitment companies however, it reduces risk and it is likely legitimate interest would be a suitable lawful basis for you to rely on in combination with the consent-basis relied on by the job board.

ICO have given guidance on situations where a CV is found on a job board, which makes it clear that legitimate interest would be a suitable lawful basis. See example here.

ICO Example:

An individual uploads their CV to a jobs board website. A recruitment agency accesses the CV and thinks that the individual may have the skills that two of its clients are looking for and wants to pass the CV to those companies.
It is likely in this situation that the lawful basis for processing for the recruitment agency and their clients is legitimate interests.

The individual has made their CV available on a job board website for the express reason of employers being able to access this data. They have not given specific consent for identified data controllers, but they would

clearly expect that recruitment agencies would access the CV and share with it their clients, indeed, this is likely to be the individual's intention. As such, the legitimate interest of the recruitment agencies and their clients to fill vacancies would not be overridden by any interests or rights of the individual. In fact, those legitimate interests are likely to align with the interests of the individual in circulating their CV in order to find a job.

Therefore it is reasonable to expect that the candidate has given consent for the CV to be downloaded by you – whether you download one CV or 1000 is immaterial, but for each candidate you have to ensure you can hold the data compliantly. The consent which is given to the job board will not extend to the recruitment company retaining the data for a long period so you must determine on what basis you are processing the data you have obtained, such as your legitimate interest. It is unlikely that any explicit consent given to the job board will be sufficient for all the processing you will do unless it is written by you and effectively the job board is acting as your processor (your service provider) – carrying out a role on your behalf.

Whatever legal basis you rely on however, under Article 14 GDPR, you need to tell the individual that you are holding the data.

Can we contact people on LinkedIn and download CVs from LinkedIn?

If a LinkedIn contact states they are happy to be contacted then it is likely that you will be able to rely on legitimate interests and your grounds for processing. The ICO has confirmed in their guidance available here:

ICO EXAMPLE: An individual creates a profile on a social networking website designed specifically for professional networking. There is a specific option to select a function to let recruiters know that the individual is open to job opportunities.

If the individual chooses to select that option, they would clearly expect those who view their profile might use their contact details for recruitment purposes and legitimate interests may be available (subject to compliance with other legal requirements, and PECR in particular). However, if they choose not to select that option, there is no such expectation, and their interests in maintaining control over their data overrides any legitimate interests of a recruitment agency or recruiting organisation.

Although reasonable expectations is an important factor, it does not automatically determine the outcome. Simply having warned the individual in advance that their data will be processed in a certain way does not necessarily mean that your legitimate interests always prevail, irrespective of harm. And in some cases you may still be able to justify unexpected processing if you have a compelling reason for it.

Therefore in our opinion when individuals upload data to LinkedIn they are aware through LinkedIn current terms that their data can be downloaded by third parties (unless they restrict the privacy settings).

Similar to the situation with downloaded job board data, you need to show compliance with the principles of data protection and a ground for fair processing once the personal data hits your system. The individual may

be aware that recruiters will be downloading data to process for its legitimate business purposes. However, to comply with the principles the individual should be aware of who holds their data and why.

There is a potential issue with obtaining details from LinkedIn and relying on legitimate interest as the candidate may not have actively stated they are looking to be contacted for a job role. At the same time, the following is stated in LinkedIn's privacy policy: "Our Services allow you to explore careers, evaluate educational opportunities, and seek out, and be found for, career opportunities. Your profile can be found by those looking to hire (for a job or a specific task) or be hired by you." This statement could be interpreted as the members of LinkedIn are aware of the potentiality of recruiters contacting them and that it therefore would be lawful to rely on legitimate interest.

Since there are conflicting opinions in regard to the usage of LinkedIn, there is a risk in downloading member data unless they have opted in to be found by recruiters. The processing could fall within your legitimate interest but if it doesn't and the act of contacting them is marketing, you would require consent.

What about referrals?

You must consider your relationship with the individual and whether the individual would reasonably expect the processing to occur. If you are relying on legitimate interests it is harder to demonstrate that the processing can be reasonably expected. If you obtained the data from a third party, you need to be clear what the individual was told about when that data might be passed on for use by others, and whether this covers you and your purpose for processing, as this will affect reasonable expectations. You can ensure you do this by making sure your privacy notice is sent at the earliest opportunity.

Should candidate or contractor registration forms include a consent field (e.g. your details will be added to … and shared with … and we will keep records of…)?

Any consent required should be specific e.g. to receive relevant marketing from you, to receive relevant marketing or contact from third parties or to introduce a candidate to relevant employers.

If you are relying on legitimate interest you do not want to ask for consent to process their data for work finding services.

You need to decide why and what consent you want to include on your registration form and provide a link to your privacy notice.

We have provided template consent wording for marketing in our GDPR toolkit.

Can we e-mail candidates about a different role from the one they originally applied for?

Again this depends on your lawful processing ground.

If you are relying on legitimate interest to process personal data in order to provide work finding services on the candidate's behalf then as long as the candidate would reasonably expect their personal data to be processed for a particular purpose then it should be fine.

How can we control what our suppliers and other parties do with the personal data, particularly if they are outside of the EEA e.g. Dropbox?

Understanding the data flows from your business to all third parties is an important part of GDPR compliance. Once you've undertaken a data audit and understand what data you hold the next step is to map your data flows – to your suppliers and other parties in a permanent or temporary supply chain. This will include parties such as data hosts, MSPs, your insurance brokers, umbrella companies etc.

You need to decide whether you are acting as a controller, co-controller or processor in respect of each relationship. The appropriate contractual relationships will then need to be in place with liability and indemnities apportioned.

Put very simply, it needs to be set out in a contract who does what to ensure data compliance. One party will need to provide the individual with information about the nature of the joint controller relationship, the basis of compliant processing and provide a contact name for the data subject. Under Article 26, the individual can enforce their rights against each of the controllers.

If the data is held or processed by a third party outside the EEA, either as a controller or as your processor (as in the Dropbox example) there needs to be contractual clauses in place to ensure the non EEA party controls/processes to a standard acceptable to the EU rules. In respect of the USA, this requires compliance with the EU/USA Privacy Shield programme.

You could use the following:

- standard data protection clauses in the form of template transfer clauses adopted by the European Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority such as the ICO and approved by the European Commission;
- compliance with an approved code of conduct approved by a supervisory authority such as the ICO;
- Certification under an approved certification mechanism as provided for in the GDPR.

Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. Put simply, make sure you have well drafted, fair and signed contracts.

If we operate in more than one EU member state, what do we need to do?

If your organisation operates in more than one EU member state, you should determine your lead data protection supervisory authority and document this. The lead authority is the supervisory authority in the state where your main establishment is. Your main establishment is the location where your central administration in the EU is or else the location where decisions about the purposes and means of processing are taken and implemented. This is only relevant where you carry out cross-border processing – i.e. you have establishments in more than one EU member state or you have a single establishment in the EU that carries out processing which substantially affects individuals in other EU states. If this applies to your organisation, you should map out where your organisation makes its most significant decisions about its processing activities. This will help to determine your 'main establishment' and therefore your lead supervisory authority. The Article 29 Working party has produced guidance on identifying a controller or processor's lead supervisory authority.

You should take your own legal advice if you control and process data in other EU countries.

Can an individual data subject claim damages under the GDPR?

Yes, a data subject can lodge a complaint with the ICO.

A data subject can also bring a claim for remedy in the courts under Article 79. They have a right to compensation from the controller or processor for damage suffered (Article 82).

Where more than one controller or processor is involved there is joint and several liability, meaning any one party may have to pay the compensation, even if they are not at fault. Therefore, liability between the parties must be set out in the contracts between them. In addition, the party which has paid the compensation has the right under the GDPR to claim back, from the other parties, compensation paid arising from their acts or omissions.

Does APSCo provide precedents?

APSCo provides some precedent documents available in the GDPR toolkit. The GDPR cannot be approached with a one size fits all mentality. Prior to finalising paperwork you need to understand your data – with a data audit, data mapping, internal awareness and training, documentation of your activities.

Our legal affiliates are able to deliver bespoke legal advice to your business and some other affiliates may offer precedents as part of their service offerings. You can find further details on our legal affiliate offerings here.

Are the model contracts and templates on the APSCo website GDPR compliant?

Yes. We have updated the templates to reflect the changes and requirements of the GDPR.

Do I need a data sharing agreement for my clients and/or umbrella companies?

When sharing personal data with third parties (such as RPO-companies, umbrella companies or payroll companies), there should be GDPR-compliant data sharing terms in place. This can be done either through a separate data sharing agreement or by having data sharing terms in the contract between the parties.

Additionally, you should have a policy on using data from job boards, alternatively include information on how you use job boards in a privacy notice, or similar. In each situation you need to ascertain whether you are working as a **controller**, **processor** or **co-controller** and the basis on which the other party is operating.

If someone is your **processor** must have a processor agreement. The processor agreement is a legal requirement and is not to be confused with the data sharing agreement. You can have either a separate data processor agreement or include data processor terms in the contract between the parties.

If you are **co-controllers** you may need a data sharing agreement although, even if you do not need one, it might be helpful for you to know what you are data sharing.

In a normal tripartite relationship with an umbrella, recruitment company and client you will all be a **controller** in your own right.

In the recruitment sector, who is likely a processor and therefore someone we need a processor agreement with?

If you are acting as an MSP then you may well be acting as a processor and that needs to be defined. Payroll providers may also be a processor but you should clarify this with any of your suppliers. It is unlikely umbrella companies will be a processor as they also control their own data.

Data processors have direct responsibility for their own compliance with the GDPR, with potential sanctions and other consequences of non-compliance.

Is it OK to pass on payment information to a contractor or umbrella company when they ring up?

Our advice is that information should only be disclosed in writing, because it will otherwise be difficult to keep track on to whom or whereto the data is provided.

The GDPR requires that you only pass on information when you have a legal basis to do so and that you pass on information transparently, i.e. the contractor must be aware that his or her data might be shared over the phone.
If you are going to provide payment data to a contractor over the phone you must first establish that the person on the phone is who they say they are. Therefore, we would suggest that you set up a checking system. With regard to providing information to a third party, the above issue regarding security of who you are speaking to still applies.

Do we need to send out communication to our whole database?

The GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. Data controllers are expected to take 'appropriate measures' in ensuring that the data subjects receive the information that they are entitled to. Therefore, you might decide that it is appropriate to contact your database to highlight your GDPR privacy notice. Please note that this is different from contacting your database to obtain consent.

Email Footers - do we legally have to mention GDPR or include an Opt-Out in our email footers?

You don't have to mention that you are GDPR compliant. The GDPR is a law and must be abided by. However, being transparent and providing accessible information to individuals about how you will use their personal data is a key element of the GDPR. The most common way to provide this information is in a privacy notice. It can therefore be good practice to link or refer to you privacy notice in a footer, as well as provide an opt-out for any service that require opt-ins.

Does APSCo provide guidance processing employee data? Will we need to update our employment contracts?

Employers who rely upon an employee or prospective employee's consent to data processing in their employment contracts must take note: Consent is not an appropriate ground for employee data. Those clauses will fall foul of the requirement that consent be freely given, due to the imbalance of negotiating power. Furthermore, consent clauses in an employment contract are not distinguishable from other matters. Under the GDPR employers can rely on processing being necessary for the performance of the employment contract. You must still think carefully about all the uses you make of their data from running the payroll to posting pictures of staff on your website when considering the wording of consent.

For new hires, you should replace the consent language in these documents by new language referencing one or more of the alternative legal bases or alternatively it might be a better idea to just refer to your privacy notice. For existing employees, companies will need to roll out employee privacy notices which refer to these alternative legal bases and inform the existing employees.

What do we need to explain to our internal employees about the GDPR?

You should make sure that decision makers and key people in your organisation are aware of the data protection laws (both GDPR and DPA 2018). They need to appreciate the impact data protection has and identify areas that could cause compliance problems under the GDPR. Go through your organisation's risk register, if you have one, and always do a risk assessment before you implement new procedures.

Your employees and consultants have a great deal of responsibility over your data so they need to be aware of the impacts and the general requirements to comply with the GDPR and the DPA 2018. APSCo has produced template GDPR-slides to help you to train your employees. These are available in the GDPR toolkit.

I am unsure if the security measures my organisation has in place are sufficient. What happens if we suffer a breach?

The GDPR includes provisions that promote accountability and governance. There is also a duty to implement measures to ensure a level of security which is "appropriate to the risk". This means that your company procedures, the operating systems and other software that you use as well as staff training needs to be assessed in order to decide on the sufficiency of your security.

Your organisation should be clear about the information it holds, where and how it is stored, and who the information is being shared with. For training purposes, your social media policies should be clear and robust to make it clear what recruitment consultants can and cannot do with client and candidate data.

Should your organisation suffer a data breach, the GDPR requires the breach to be reported to the ICO within 72 hours, where possible. It is expected that action plans for both preventing and responding to data breaches are put in place by your organisation.

One of the significant ways in which an organisation can look to further safeguard personal data is to implement a Data Protection Impact Assessment ('DPIA'). Organisations should look to implement a DPIA when processing data in way that is new or has a perceived risk to the information.

How long can I keep personal data for and do I need a retention policy?

Personal data should be kept for no longer than necessary for your legitimate business purposes. This must always be considered in light of the individuals' rights and their expectations when you collected the data.

Therefore, keeping personal data indefinitely without periodically reviewing your continued need for it is not acceptable. All recruitment businesses will need retention policies and processes for periodically cleansing data.

Candidates', contractors' and prospect data are all held for different purposes and the length of time you can legally retain their data will differ. Neither the DPA nor the GDPR gives minimum or maximum periods for the retention of data. Both legal documents state that personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose(s). The following should be considered:

- the purpose(s) for which the data is kept;
- how to keep data up to date;
- how long it is necessary to retain data for that purpose(s);
- to have a process to securely delete data, the retention of which is no longer necessary; and
- to update, archive, or securely delete data which goes out of date.

Therefore, you will need to retain different data for different periods of time. For example, if the data is being kept to defend a claim in contract or tort, statute of limitations is 6 years in the UK, and you might therefore be able to retain the data for 6 years. The same is true for accountancy records. However, in other cases it may not be reasonable to retain data for longer than a few weeks. For example, candidate CVs that you do not end up putting forward to a client.

You will need to make an assessment by type of data weighing up how long is reasonable for your legitimate business purposes, taking the individual's expectations into consideration. Your retention policies should be summarised in your privacy notice. Additionally, if the individual gives consent for you to process his or her data, the individual needs to be informed about how long the data will be retained for (or the criteria you use to make that decision) at the time of them giving consent.

You can review out Retention Analysis Table in the GDPR toolkit which is a starting point to help you think about the categories of personal data you hold and how long you need it for. You will need to devise the right retention plan for your own business. This is not something that a template can be provided for.

What is the standard retention period for a recruitment company?

The GDPR does not outline specific retention periods for the different categories of personal data. However, the principles of the GDPR say data needs to be adequate, relevant, and kept for no longer than is necessary for the purposes for which it is being processed. This means, as a data controller, you will need to consider the personal information you hold and determine if the retention period applied is appropriate.

Should we have different retention periods for candidates we have placed compared to candidates who we have never placed?

If you haven't had any meaningful contact with a candidate (i.e. not relevant for the purposes it was collected), it would be sensible to have a much shorter retention period compared to a candidate you have placed. If you have had some contact (i.e. a link in an email is clicked on) you may decide to base your retention period from the end of this contact compared to when they were first put on your system or for such period that the Law requires. How long certain kinds of personal data should be kept may also be governed by specific business-sector requirements or statutory retention period and agreed practices.

Can we collect, use and store prospect client data from, for example, conferences and events?

You need to have a lawful processing ground for holding the data and supply a copy of your privacy notice to them as you do for candidates.

What records must we keep about our personal data processing activities?

As well as your obligation to provide comprehensive, clear and transparent privacy policies, if your organisation has more than 250 employees, you must maintain additional internal records of your processing activities.

If your organisation has less than 250 employees you are required to maintain records of activities related only to higher risk processing, such as processing of special categories of data (sensitive data) or criminal convictions and offences. However, we recommend that you record the data below as best practice, even if at a higher level, so that your board understands the scope of your processing and so that you can respond adequately to an investigation by the ICO.

What records must I keep if my organisation has more than 250 employees?

You must maintain internal records of processing activities. You must record the following information:

- Name and details of your organisation (including (where applicable) other controllers, your representative and DPO).
- Purposes of the processing.
- Description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data.
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- Description of technical and organisational security measures.

What is a personal data breach and when does it have to be notified?

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

The ICO GDPR-overview states that not all breaches need to be notified to the ICO– "only if a breach is likely to have a significant detrimental effect on individuals"– for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. This has to be assessed on a case by case basis. For example, you will need to notify the relevant supervisory authority about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold. Individuals must be told if there is a "high risk" to their rights.

"A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority."

What must a data breach notification contain?

The nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned; and
- The categories and approximate number of personal data records concerned;
- The name and contact details of the DPO (if your organisation has one) or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

How do I notify a data breach?

A notifiable breach has to be reported to the relevant supervisory authority (the ICO in the UK) within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.

If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.

Failing to notify a breach when required to do so can result in a significant fine up to €10M or 2% of your global turnover.

What does data protection by design and by default mean?

Put simply you need to show you have considered and integrated data protection into your activities and consider data protection as a default item when introducing new activities, processes and systems into your business.

What is a data protection impact assessment and when are they needed?

Data protection impact assessments (DPIAs) (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations. You must carry out a DPIA when using new technologies which may involve systematic and extensive processing activities, including profiling and/or large scale processing of special categories of data or personal data in relation to criminal convictions or offences and/or large scale systematic monitoring of public areas (CCTV). This is a non-exclusive list and it will be sensible to conduct a PIA for any larger scale changes to your systems and processes.

The ICO have given guidance on conducting privacy impact assessments under the DPA 1998 and have a template privacy impact assessment. You can find this in our GDPR toolkit.

What information should a DPIA contain?

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.
- A DPIA can address more than one project.

What are the Individuals' Rights under data protection laws?

1. The right to be informed (see Part 1 How Can I Process Data Compliantly)
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

What is the Right of Access?

Under the GDPR, individuals will have the right to obtain confirmation that their data is being processed, to access their personal data and to receive other information largely corresponding with the information that should be provided in a privacy notice – this is called a Subject Access Request.

How do I handle a Subject Access Request?

You must provide a copy of the information free of charge. You can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive or for requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests. The fee must be based on the administrative cost of providing the information.

You will have less time to comply with a subject access request under the GDPR. Information must be provided without delay and at the latest within one month of receipt. You will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

You can refuse to respond if the request is manifestly unfounded or excessive, in particular repetitive. Where you refuse to respond to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

You 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. Where possible, the individual should be provided with remote access to a secure self-service system allowing direct access to their information (without adversely affecting the rights of other individuals).

There is no exemption for requests relating to large amounts of information held across multiple systems but you could consider whether the request is manifestly unfounded or excessive.

How can I be confident I am handling Subject Access Requests correctly?

Train staff to record information on individuals succinctly and accurately, make them aware the data is not private as the individual has the right to see it and avoid recording subjective opinion on an individual unless it is relevant to the services you are providing e.g. feedback on a candidate following an interview.
Speak to your system providers about how you are best able to interrogate your data and consider other sources of data e.g. employee records, system testing data and how this can be accessed effectively.
Consider using specialist tools such as keyword software, which for example can remove duplicates from an email chain.

Audit your responses to SARs on a periodic basis (subject to the volumes you receive) in terms of compliance with deadlines, quality of personal data disclosed and format of disclosure.

What is the Right of Rectification?

Individuals are entitled to have personal data corrected if it is inaccurate or incomplete.

If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

You must respond within one month to a request to rectification. This can be extended by two months where the request for rectification is complex.

You can refuse to rectify data, but you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

What is the Right to Erasure or the Right to be forgotten?

An individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing.

When does the Right to Erasure apply?

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.

When can I refuse to comply with a Request for Erasure?

You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
- the exercise or defence of legal claims.

You can also defend your right to retain the data on the basis it is still necessary for the purpose for which it was originally collected or there is an overriding legitimate interest to continue the processing. Note the individual has stronger rights if the processing is carried out on the ground of consent as the individual can withdraw consent at any time. You have to erase the data unless there is an alternative legitimate ground for processing.

There is also the practical difficulty of ensuring that the individual is not re-entered on your system as a new record after erasure. It is therefore worth considering whether any technical identifier could be embedded in your system to prevent this happening or at least flag it as an issue.

See below the Right to Restrict Processing, which might be a valid alternative to complete erasure of the personal data.

Do I have to tell other organisations about a Request for Erasure?

If you have disclosed the personal data in question to third parties, you must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. This could include your suppliers, clients and other third parties. Likewise, third parties such as LinkedIn need to consider their duties to notify you of a Request for Erasure.

The GDPR reinforces the right to erasure by clarifying that organisations in the online environment that make personal data public should inform other organisations who process the personal data to erase links to, copies or replication of the personal data in question.

The ICO acknowledges that in practice is challenging particularly for online controllers and processors. There is little precedent as this is a far broader right than under the DPA 1998.

Always document your response to the individual, particularly if you are unable to fully execute the erasure, and are relying on a ground to retain the data; are refusing to comply for one of the reasons listed above; or are not informing all third parties due to disproportionate effort.

Can I keep a suppression list to avoid contacting individuals who have asked to be erased?

In some cases you may need to keep a record of the erasure request – for example, to maintain suppression records so that you can comply with direct marketing rules. You don't need consent for this, as long as you tell the individual in question that you will keep these records, why you need them and your lawful basis for this processing (e.g. legal obligation or legitimate interest).

Instead of deleting an individual's details entirely, suppression involves retaining just enough information to ensure that the individual's preferences are respected in the future. Suppression allows organisations to ensure that they do not send marketing to people who have asked them not to, as there is a record of the request. If people's details are deleted entirely, there is no way of ensuring that they are not put back on the database. Deleting details might also breach industry-specific legal requirements about how long to hold personal data.

You may not contact an individual on a suppression list at a later date, in order to ask them if they want to opt back in. Contacting someone on a suppression list is likely to breach the DPA and will also breach PECR if the contact is by phone, text or email.

What is the Right to Restrict Processing?

Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

When does the Right to Restrict Processing apply?

You will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests) and you are considering whether your organisation's legitimate grounds override those of the individual.

- When the processing does not comply with the GDPR and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If you have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so. You must inform individuals when you decide to lift a restriction on processing.

How will the Right to Data Portability affect our data?

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability e.g. price comparison quotes.

However, the right to data portability only applies:

- To personal data an individual has provided to a controller;
- Where the processing is based on the individual's consent or for the performance of a contract; and
- When processing is carried out by automated means.

Therefore, unless you conclude you carry out processing by automated means, it is unlikely this right will apply to your organisation at all.

Examples of automated and non-automated decision making given by the ICO under the DPA:
Automated Decision based on automated processing: A factory worker's pay is linked to his productivity, which is monitored automatically. The decision about how much pay the worker receives for each shift he works is made automatically by reference to the data collected about his productivity.
However, please note that agency workers and professional contractors usually work on a time and materials basis and that generally time has to be entered into a system and approved by **people**, even though it may then be processed by an automated billing system without further human intervention.

Non-Automated Decision based on partially automated processing: An employee is issued with a warning about late attendance at work. The warning was issued because the employer's automated clocking-in system flagged the fact that the employee had been late on a defined number of occasions. However, although the warning was issued on the basis of the data collected by the automated system, the decision to issue it was taken by the employer's HR manager following a review of that data. So the decision was not taken by automated means.

How should I comply with the Right to Data Portability if applicable?

You must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The information must be provided free of charge and you must respond within one month. The response period can be extended to two months if the request is complex or if there are multiple requests.

If the individual requests it, you may be required to transmit the data directly to another organisation if this is technically feasible. However, you are not required to adopt or maintain processing systems that are technically compatible with other organisations.

If the personal data concerns more than one individual, you must consider whether providing the information would prejudice the rights of any other individual. Where you are not taking action in response to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

When does the Right to Object to Processing apply?

Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

You should offer a way for an individual to object online, if any of your processing is carried out online. You must highlight the Right to Object to Processing in your Privacy Notice.

You should stop processing the data upon receiving an objection unless your legitimate business grounds for processing overrides the individual's rights or the processing is in respect of legal claims.

You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse. You must deal with an objection to processing for direct marketing at any time and free of charge.

Is the Right to Object to Automated Processing and Profiling relevant to us?

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. Individuals have the right not to be subject to a decision when:

- It is based on automated processing; and
- It produces a legal effect or a similarly significant effect on the individual.

You must ensure that individuals are able to obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

The right does not apply if the decision is necessary for entering into or performance of a contract between you and the individual, is authorised by law (e.g. for the purposes of fraud or tax evasion prevention) or based on explicit consent.

Is the Right to Object to Profiling Relevant to us?

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

- Performance at work;
- Economic situation;
- Health;
- Personal preferences;
- Reliability;
- Behaviour;
- Location; or
- Movements.

When processing personal data for profiling purposes, you must ensure that appropriate safeguards are in place:

- Ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences.
- Use appropriate mathematical or statistical procedures for the profiling.
- Implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions taken for the purposes listed in Article 9(2) must not be based on the processing of special categories of data unless you have the explicit consent of the individual.

You particularly need to consider whether you undertake automated decision making and/or profiling of your employees as well as candidates or clients.

Should you require further advice please contact the legalhelpdesk@apsco.org