# Data Protection and Privacy Policy

This policy comprises of this Data Protection and Privacy Policy and the following Appendices:

1. Data Sharing Policy
2. Supplier Due Diligence Policy and Questionnaire
3. Subject Access Requests Policy
4. Individuals Rights Policy
5. Breach Management Policy
6. Data Retention Policy
7. Strong Password Policy
8. Data Protection Impact Assessment Policy

## 1. Purpose

This Data Protection and Privacy Policy defines the way in which Elior UK (which includes as at the date of this Policy, Lexington, Taylor Shaw, Caterplus and Edwards and Blake) (referred to in this Policy as the **Company**, **we** or **us**) operates to ensure compliance with data protection legislation in the UK. It sets out the standards with which all Company colleagues and contractors (referred to in this Policy collectively as **colleagues** or **you**) must comply when handling personal data.

## 2. Background

The Company needs to collect and use personal data about colleagues, customers, consumers and other individuals with whom we come into contact for a variety of purposes. The UK General Data Protection Regulation tailored by the Data Protection Act 2018 (**UK GDPR**) places obligations on organisations that use personal information and gives individuals certain rights. The UK GDPR requires the Company to be open about how personal data is used and to follow various principles to protect personal data. As the Company also, in certain sites where we operate, undertakes direct marketing to consumers the Company and its subsidiary entities are also required to comply with the Privacy and Electronic Communications (EC Directive) Regulations 2003 which sits alongside the UK GDPR (**PECR**) which govern direct marketing by electronic means.

## 3. Scope

This Policy applies to all of our colleagues whenever you collect, use, access or share "personal data" relating to customers, colleagues, suppliers, consumers or other individuals.

- "Personal data" means any information about an identifiable living individual. This includes, for example, an individual's contact details, such as name, address, email address and telephone numbers. It can include information about individuals' opinions and beliefs too. In relation to colleagues, personal data includes job role, salary and benefits information and performance reviews.
- "Special categories of personal data" (**SCPD**) are types of personal data which are more sensitive than usual and require additional protections. These include information relating to an individual's racial or ethnic origin, gender, religious beliefs, philosophical beliefs, physical or mental health, sexual life and trade union membership. We have to take extra steps to ensure compliance with legal obligations when we process SCPD.
- "Criminal conviction data" also requires further protection and must only be processed in limited circumstances.
- Financial information, such as bank account and credit card details, is not designated as SCPD but we must take extra care when collecting, processing and storing financial information. This is because if the information falls into the wrong hands, it could be used to commit fraud or identity theft.

We handle personal data all the time in order to run our businesses, for example:

- when line managers and HR teams collect information about colleagues in order to make salary payments and carry out performance reviews;
- when we collate mailing lists and use these to send direct marketing to individuals;
- when we collect information about any individuals' medical requirements to provide them with appropriate meals;
- when we capture images of colleagues and other individuals on CCTV cameras; and
- if customers or clients contact us with any problems, queries or complaints.

# Data Protection and Privacy Policy

## 4. Responsibilities

We have various responsibilities under the UK GDPR. This section sets out what those responsibilities are and how you must help to ensure that we meet those responsibilities.

A. Transparency and fairness

We must be clear and open about what we intend to do with individuals' personal data. This ensures that individuals feel comfortable that their personal data is safe with us and we will not use it in any ways that are unfair, incompatible with the purpose for which the data was collected or that would not be anticipated by the relevant individuals.

Therefore, before we collect personal data, we must explain to the relevant individuals in plain language:

- who we are;
- what personal data we are collecting about them and where we get this from;
- what we are going to do with their personal data and our legal justification for doing this;
- whether we are going to share their personal data with anyone else;
- how long we are going to hold their personal data for;
- whether we are going to transfer any of their personal data overseas; and
- what rights those individuals have in relation to their personal data.

We communicate this information to individuals in specific privacy notices for each category of individual. For example, the Elior Colleague Handbook, MyView dashboard and the Company extranet provide information to colleagues about how we use colleagues' personal data. Our clients may provide privacy notices to individuals whose personal data they collect and pass on to us to process, for example where we need to collect information about medical conditions to ensure that we provide individuals (for example, pupils or residents in care homes) with safe meals.

We must also ensure that our processing of personal data is "fair". This means that we must always have legitimate reasons for collecting and processing personal data and must not use it in overly intrusive ways. The most common reasons are:

- for colleague personal data, to manage and administer employment contracts, comply with employment laws and monitor equality and diversity; and
- for consumer personal data, to provide our services and (where SCPD is processed) based on the consumer's consent or for the purposes of fulfilling other requirements such as legal or regulatory obligations.

B. Keeping data accurate and up to date

To ensure that our records are accurate and up to date in accordance with the Data Retention Policy at Appendix 6, we must:

- check that information is correct when we first receive it;
- periodically review the personal data that we hold to ensure it remains up to date; and
- correct inaccurate data as soon as possible.

If we receive a request to correct inaccurate information, we must:

- promptly comply with the request (if appropriate to do so);
- check that the individual is who they say they are by running appropriate identification checks; and
- take reasonable steps to confirm the accuracy of the information provided (for example, if you receive a request by email to correct personal data, by telephoning the individual to confirm the details provided).

If you believe a request to correct inaccurate data is dishonest or inaccurate, please refer this to your line manager in the first instance.

## Data Protection and Privacy Policy

As one of our colleagues, it is important to us that we ensure we are processing accurate information about you as well. Therefore, if you think any of the data we hold on file about you is inaccurate, please refer this to your line manager.

We must also take steps to minimise the personal data that we handle and make sure that we are not processing any more personal data than is strictly necessary to fulfil the purposes of the processing. For example, we may need to process information about an individual's medical condition to provide them with a safe meal, but we will not need to collect information about that person's race for that purpose. If you think that we are using any personal data which we do not need to use, please refer this to your line manager.

C. Keeping data secure

We take data security very seriously and all personal data we use must be kept secure at all times. Failure to keep data secure can lead to real harm and distress for individuals, for example:

- credit card fraud or identity theft in the case of financial information;
- harm to a person's career in relation to HR data;
- risk of physical harm if address information is released to the wrong person; and/or
- in all cases, the risk of a breach of a person's privacy rights.

There are a number of ways to protect personal data stored on electronic or hard copy files. For example:

- Authentication systems: All files which are either (1) sent by the HR department; or (2) sent by any department or function which contain personal data of any kind; either internally or externally, will be password protected with a Strong Password and the Strong Password will be sent to the recipient via an alternate means to the files which are sent (i.e. if files are emailed, the Strong Password will be sent via Microsoft Teams or a text message).
- Strong Passwords: You must comply with our Strong Password Policy at all times to ensure that your passwords are robust and can only be reset by yourself through your previously registered information.
- Limiting staff access: You should only be able to access data which you need to access in order to perform your work duties. If you believe you have access to more information than is required, please advise your line manager.
- Don't leave devices unattended. If you need to leave a device unattended, for example to go to the printer, you must make sure that electronic files are inaccessible. For example, computers and wireless devices must be screen-locked and password protected. Hardcopy files containing personal data should not be left in open view.
- Portable devices: Personal data stored on mobile devices (e.g. notebooks, iPads, memory sticks), laptop computers and mobile phones is also subject to this Policy. Great caution must be used when storing data in this way. These devices must always be encrypted and any use of such device or synchronisation tools used with such devices must be in accordance with our IT policies.
- Paper records: Remember that paper or hardcopy, as well as electronic files, can include personal data, so you need to ensure that paper files and records are stored and disposed of securely e.g. stored in a locked cabinet when not in use and shredded before disposal in accordance with our Data Retention Policy.

D. Sharing personal data

When we share personal data outside of the Elior UK group, we must be clear and open about this with the relevant individuals and tell them why we need to do this in our privacy notices. In particular, the following requirements must also be met:

*Sharing personal data with the police and regulators:*

- We are sometimes contacted by the police, local government, regulators, banks and other organisations requesting personal data to assist them with crime prevention and detection, fraud investigations and to verify information relating to credit and job applications.
- We cannot automatically provide such information and may only do so in certain circumstances and in accordance with our Data Sharing Policy at Appendix 1. If we breach those obligations, we could face

enforcement action such as fines, claims for compensation from individuals affected and reputational damage. Therefore it is important that we are very careful about what personal data we send to third parties and why. If you receive any request to release information, please refer to the Data Sharing Policy and please speak to your line manager before releasing any information to the person making the request.

*Sharing personal data within the Elior group:*

- The same rules apply if we wish to share personal data within the Elior group of companies. We are not permitted to pass personal data to other group companies unless we have previously told the individuals that we will do so, the individuals have consented for us to do so or we are permitted to share data under a legal exemption, for example for crime prevention and detection purposes or to defend our legal rights.
- In particular, if we wish to pass personal data to another Elior group company for marketing purposes, we must have express consent from the individual to share personal data with group companies in this way.
- If you receive a request to transfer personal data to another Elior company and you are unsure whether you are permitted to do so, please refer to your line manager in the first instance.

*Sharing personal data with suppliers:*

- If individuals would reasonably expect us to share personal data, we will be permitted to do so as long as the sharing is for a legitimate business purpose. For example, this would include passing personal data to our suppliers to enable them to provide services to us, such as providing payroll providers with colleague salary and bank details to enable monthly salary payments to be made.
- When we pass personal data to third party suppliers who use the data to provide services to us, we must ensure they have adequate measures in place to keep personal data secure and we must ensure that a written contract is in place with the supplier. This means that we need to carry out due diligence on suppliers before providing them with any personal data to ensure their systems and procedures are adequate to keep personal data safe and to enable compliance with individuals' rights and other UK GDPR requirements (refer to the Supplier Due Diligence Policy and Questionnaire in Appendix 2). The Legal Department (working in conjunction with the Purchasing Department) will ensure that the contract that is put in place imposes a number of specified data protection obligations on the supplier, including an obligation to keep personal data secure and to only process personal data in accordance with our instructions.

*Transferring personal data overseas:*

- We cannot send personal information, or allow people to access personal information, outside the UK and the EEA unless certain additional requirements are met, for example UK approved model contract clauses are in place. If you are working on a project that might involve sending personal information outside the UK (for example, using cloud storage in the USA) and if you are unsure about whether you have met these conditions, you must refer to your line manager.

E. Individuals' rights

Individuals have a number of rights in relation to their personal data and we must comply with requests to exercise those rights in the circumstances set out in data protection legislation. More detail about these rights can be found in the Subject Access Request Policy at Appendix 3. Briefly, these rights include:

- A right to ask for a copy of all personal data we hold about an individual;
- A right to ask for a machine-readable copy of information an individual has provided to us;
- A right to ask us to delete personal data in certain circumstances;
- A right to ask us to restrict processing of personal data in certain circumstances;
- A right to object to us processing your personal data in certain circumstances;
- A right to ask us to correct inaccurate personal data;

## Data Protection and Privacy Policy

- A right to opt out of direct marketing; and
- A right to request that any wholly automated decisions made about an individual which cause legal or significant effects for them are reviewed manually.

F. Think privacy

When we start any new projects that involve personal data or we wish to use personal data in a new or different way, we need to ensure that the privacy risks have been assessed and addressed properly from the outset. This means we need to do two things:

- Consider privacy risks when we start new projects involving personal data. This involves identifying the key personal data risks that may arise in relation to a particular project, include legal risks, reputational risks and risks to individuals. For high-risk data processing, we must carry out a "Data Protection Impact Assessment" or "DPIA" which enables us to identify these risks and mitigating actions. Please refer to our Data Protection Impact Assessment guidance on the extranet for more information.
- Ensure that when we design projects, journeys or processes, we use "privacy by design" principles. This means that privacy is embedded into procedures and systems from the outset of the project. When building new systems, products or procedures, we should bear in mind privacy considerations and ensure that privacy is maximised.

G. Marketing

We are committed to compliance with PECR in relation to direct marketing by electronic means, in particular:

- ensuring that the relevant individuals have given express opt-in consent;
- ensuring that the marketing communication reminds individuals that they can prevent further marketing by a simple and free method; and
- ensuring that no single recipient will see the names and contact details of any other recipient.

This means that when you are sending electronic direct marketing communications (e.g. by email, text or phone), you must not do so unless you are sure that we have consent from all the recipients to receive those marketing communications. Every marketing communication must include an "opt out" option for individuals which should be easy and free, for example by clicking an "unsubscribe" link in a marketing email. When communications are sent out, no individual email addresses should in the "To" or "CC" email boxes. Instead, you should make sure that individual addresses are included in the "BCC" box or that the communication is sent to a named mailbox which does not identify particular individual email addresses.

H. Breaches

Despite all our best efforts, issues may sometimes arise. For example:

- we may lose personal data accidentally;
- someone may steal personal data or attack our systems;
- one of us may not be authorised to use personal data; or
- our IT equipment may fail.

If we suffer a security breach, we have to act immediately in order to manage the breach and limit the effects and damage it causes. We may also need to tell the data protection regulator and/or the individuals affected that the breach has occurred so it is important that breaches are dealt with as quickly and efficiently as possible.

If you suspect or become aware of a data security breach, please follow the steps set out in our Breach Management Policy at Appendix 5 to enable us to respond appropriately.

I. Penalties

Breaches of data protection law can have grave consequences in terms of real harm and distress for the individuals affected. They can also lead to serious consequences for us, including:

- fines from the data protection regulator of up to £17.5 million, or 4% of annual global turnover, whichever is greater;
- individual compensation claims from the individuals affected; and
- reputational damage and loss of customer, consumer and colleague trust.

It is therefore essential that you comply with the requirements of this Policy and escalate any breaches in accordance with the Breach Management Policy. Failure to do so may lead to disciplinary action.

**5. Medical diet information for children**

Sometimes we will need to process SCPD about primary school children when we are providing catering services in primary schools and we need to know medical information about children to provide them with a safe medical diet. We must be particularly careful with this information because the information being collected will be very sensitive and relates to children. We will also need to ensure that our clients have obtained requisite parental consent to the use of any SCPD about children.

If you are processing SCPD about children for these purposes, you must ensure that our standard template Medical Diet Request Form is used by the client (or a similar document is used based on the client's standard template to obtain similar information). This Form is available from the Legal Department and includes wording for the school to obtain parental consent to the use of information by us about the child's medical condition for the purposes of providing a medical diet.

You must also ensure that clients are using the Medical Diet Parent/Carer and Child Privacy Notice to provide these documents to parents/carers along with the Medical Diet Request Form. This Privacy Notice is available from the Legal Department.

**6. Governance and changes to policy**

The Elior UK Legal and Compliance will review ongoing compliance with the UK GDPR on a quarterly basis with Group Elior Compliance Officer. This Policy is reviewed at least annually at Board level and will be revised in accordance with our procedures and any changes in legislation.

**7. Further information**

If you have any queries relating to this Policy or would like further guidance on any of the matters covered in it, please contact your line manager in the first instance.

**Catherine Roe**
Chief Executive, Elior UK
14 December 2022

# Data Protection and Privacy Policy

**Appendix 1**

**Data Sharing Policy**

## 1 Purpose

1.1 This Data Sharing Policy sets out how you should treat requests received from third parties for copies of someone's personal data. If you receive a request from an individual for his or her own data, please refer to the Subject Access Request Policy at Appendix 3.

1.2 This Protocol is intended to apply to one-off requests for information. If you have received a request from a third party to enter into an ongoing data sharing arrangement, please refer this to the Legal Department.

1.3 If you are not sure how to handle a request, please speak to your line manager or the Legal Department.

## 2 Sharing personal data

2.1 "Sharing" personal data means providing or disclosing data in any form or by any means, including telling somebody orally over the phone or in person; sending information by email, text or other online messaging service; enabling access to electronic information (for example through an internet portal); and providing information in hardcopy form.

2.2 Personal data held by the Company must only be shared in accordance with this Policy.

## 3 General principle

3.1 Our starting point should always be that personal data should not be disclosed to anyone who the information is not about. Personal data is private to the individual to whom it relates and often individuals would not expect us to provide personal data about them to other people without their consent.

## 4 Sharing for limited purposes

4.1 We may be able to share personal data with third parties if:

4.1.1 the sharing is for purposes that we have told the individual about; and

4.1.2 we have told the individual that their data will be shared, or the individual would reasonably expect their data to be shared for these purposes.

4.2 For example, we may need to share personal data with our pension provider to enable our colleagues' pensions to be administered. We are allowed to do this provided we have told our colleagues that their data will be used for the purposes of administering pensions and other benefits, as colleagues would reasonably expect us to have to share data with a provider for this purpose.

4.3 In order to establish whether you can share data in this way, you should therefore look at the privacy policy or other privacy information that has been provided to the individual whose data you are proposing to share. If that information does not cover sharing for the purposes at hand, you will need to inform the individual that you are going to share their data for these purposes.

## 5 Sharing with consent

5.1 If you want to share personal data with a third party:

5.1.1 for purposes other than purposes we have already told the individual about;

5.1.2 in circumstances where the individual would not expect their personal data to be shared; or

5.1.3 where the data involved is special category personal data (for example, medical information, information about race or religion or information about political opinions or trade union membership).

you will need to obtain the consent of the individual to whom the personal data relates before you share the personal data.

5.2 When you obtain consent, you should make sure that the individual knows exactly what they are consenting to. This means giving a very clear description of who the personal data will be shared with and why.

5.3 You must make sure that consent is recorded somewhere that is clear and easily accessible in our systems. This is so that if we are ever challenged on our decision to share personal data, we can demonstrate that appropriate consent was obtained.

5.4 Remember that individuals can withdraw consent at any time. If someone changes their mind before you share the personal data, you must not share it. If someone changes their mind after you share the personal data, you may need to take steps to retrieve the personal data. Please contact the Legal Department for more information.

## 6 Legal obligations to share Personal Data

6.1 There may be certain situations when we are under a legal obligation to share personal data. For example, if someone has obtained a court order or a warrant which requires us to share personal data, then we must do so otherwise we will be in breach of our legal obligations.

6.2 However, we must only disclose the minimum amount of personal data that is required by that legal obligation. For example, if a court order requires us to share someone's name and phone number, we shouldn't also share their postal address.

## 7 Exemptions

7.1 As well as legal obligations, there are certain exemptions that we can rely on to enable us to share personal data. These exemptions allow us to share personal data without obtaining consent and without telling the individual, as long as the data is required for certain purposes.

7.2 The main exemptions are as follows:

7.2.1 We can share personal data with a third party where it is necessary to do so for the purposes of preventing or detecting crime, or for apprehending or prosecuting offenders. These types of requests are likely to come from the police and relate to ongoing investigations; and

7.2.2 We can share personal data with a third party where it is necessary to do so for the purposes of legal proceedings, obtaining legal advice, or otherwise exercising, establishing or defending legal rights. These types of requests are likely to come from solicitors or from other third parties who are intending to take proceedings against an individual.

7.3 If you receive a request from a third party and you think it might fall under one of these exemptions, you should make sure that the request is made in writing and you should send the request to the Legal Department immediately. The third party requesting the data will need to tell us the reasons why the

information requested is necessary for those purposes and we will need to make sure that we are satisfied that the information is, in fact, necessary. If you are not sure that the information is necessary, **you must not share the personal data.** You can tell the requester to obtain a court order for disclosure of the information if there is any doubt as to whether we should share the information.

## 8 Verification of identity

8.1 Even if you have someone's consent to share their personal data or there is an exemption or a legal obligation, you should always verify the identity of the person making the request so that you don't inadvertently share personal data with someone else.

8.1.1 **Individuals:** Other individuals may request data relating to someone else. For example, a teacher may request information relating to the medical diet of a child. You should make sure that you know who the requester is, the relationship that he or she claims to have with the person about whom information is requested and that he or she is entitled to have the information (for example, because there is a power of attorney or letter of authority in place).

8.1.2 **Authorities:** Sometimes the police or HMRC might ask us for information to assist with crime prevention or tax collection. For example, the police might ask us for the telephone number of someone that they suspect of fraud. You should take steps to verify the identity and job title of the person, for example asking for a work email address, checking with the relevant police force or finding a generic telephone number for the authority online and contacting the requester that way.

8.1.3 **Third party companies:** If you receive a request from a third party company, for example because the individual has applied for a job there and the request is for a reference, you should verify that the company exists and that the person making the request works there and has the job title he/she says he/she has.

## 9 Minimisation of Personal Data

9.1 Even where a decision is taken to share personal data with a third party, we must always remember that we have an obligation to make sure that the minimum amount of personal data necessary is processed, which includes sharing with third parties. Therefore, you should only disclose the minimum amount of personal data that is necessary for our or the third party's purposes.

9.2 For example, if the police request someone's telephone number as that person is suspected of fraud and the police need to track that person, you may be able to disclose the telephone number but you should not disclose other information such as that person's address or personal details, even if you think it would be helpful to do so.

## 10 Transmission of Personal Data

10.1 As well as our obligations in terms of sharing personal data, we also have obligations to keep personal data secure. This means that when you share personal data with third parties, you should do so in a way that is technologically and physically secure.

10.2 All files which are either (1) sent by the HR department; or (2) sent by any department or function which contain personal data of any kind; either internally or externally, will be password protected with a Strong Password and the Strong Password will be sent to the recipient via an alternate means to the files which are sent (ie. if files are emailed, the Strong Password will be sent via Microsoft Teams or a text message). The same principles apply to files which contain information which is commercially sensitive or highly confidential.

10.3 If data is provided in hardcopy, this should either be physically handed to the recipient or sent by recorded delivery and marked "confidential".

10.4 Always make sure that you send the personal data to the correct person. If sending electronically, check that you have put in the correct email address and do not cc other recipients. If you need to send emails to a number of individuals at the same time, always use the bcc function. If you hand the personal data to someone in hardcopy, check their ID and if you post hardcopy information to someone, make sure it is signed for by the right person.

## 11 Recording your decision

11.1 If we are ever challenged by an individual or the regulator on sharing personal data, it is important that we are able to demonstrate that the sharing was compliant with data protection laws. We must therefore make sure that there is an appropriate audit trail and keep records of data disclosed and the rationale for it.

## 12 Sharing Personal Data with suppliers

12.1 If we need to share personal data with any third party suppliers who will use that personal data for the purposes of carrying out services on our behalf (rather than for their own purposes), we can normally do this but we must conduct appropriate due diligence on the supplier or third party to assess their information security and data protection procedures before we send them any personal data. We should check that they have adequate policies and security measures in place, and that all their staff are appropriately trained on data protection. You should do this by ensuring that the supplier completes our Supplier Due Diligence Questionnaire in accordance with the Supplier Due Diligence Policy in Appendix 2. For more information, please speak to the Legal Department.

# Data Protection and Privacy Policy

## Appendix 2

## Supplier Due Diligence Policy and Questionnaire

### 1 Background

1.1 This Policy provides guidance to colleagues on appropriate due diligence we should carry out prior to contracting with third party suppliers. It also includes a Due Diligence Questionnaire which must be completed by all third party suppliers who process personal data on our behalf before entering into a contract with them.

### 2 When should I carry out supplier due diligence?

2.1 The Purchasing Department will need to carry out due diligence on a supplier when that supplier processes personal data on our behalf.

2.2 Personal data means any information relating to an identifiable living individual, which is stored electronically or within a structured manual filing system. For example, a person's contact details, payment information and online identifiers (IP and cookie identifiers) are all personal data. There is also a separate category of personal data known as 'special categories of personal data' which requires a higher standard of protection under the UK GDPR.

2.3 If information about someone is fully anonymised, so that a processing party would not be able to identify that person, this will not be personal data. However, to be "anonymous", there must be no way that the processing party can link that information back to a particular individual – you must satisfy yourself that it is impossible to link the information to a specific individual.

2.4 The processing of personal data means any operations performed on personal data such as, collection, recording, organisation, structuring, storage, adoption, use, disclosure, deletion etc. This is a very broad definition.

2.5 If you decide that the supplier is not processing personal data on our behalf, you should keep a written record of this decision and the reasoning behind it to ensure we have an audit trail demonstrating why due diligence has not been carried out. You should also make sure that you regularly review the position and the supplier's activities on an on-going basis and, if it is anticipated that the supplier will in the future process personal data on our behalf, you should follow the steps in this Policy. All on-going due diligence must be documented in writing.

### 3 Data Protection Impact Assessment ("DPIA")

3.1 A DPIA is a risk assessment undertaken to identify risks of non-compliance with data protection legislation and mitigating actions which may be employed. Where UK GDPR due diligence needs to be carried out on the third party, you should review Elior's DPIA Policy at Appendix 8 and consult with the Purchasing Department who will determine whether or not a DPIA needs to be completed by the Legal Department. If applicable, you should provide all assistance and information needed to complete a DPIA.

### 4 Supplier due diligence

**4.1** We have prepared a number of questions which must be completed by all prospective contracting third party suppliers, known as the *'Supplier Due Diligence Questions'* (the **DD Questionnaire**). The DD Questionnaire must be circulated by the Purchasing Department to the potential supplier as early as possible in the process and the contract must not be signed until the supplier has completed the DD Questionnaire to a satisfactory standard.

**4.2** There are a number of questions that should be used in all cases (referred to in this guidance note as "required questions"). There are also a number of optional questions that may be used depending on

the nature of the services. Where the handling of personal data is minimal or is otherwise low risk only the required questions will be needed. For all other contracting, the Purchasing Department will need to consider whether any, or all, of the optional questions should also be included.

4.3 When considering whether the contracting is low risk from a data protection perspective the following questions should be considered:

4.3.1 Is a large volume of personal data going to be processed by the third party?

4.3.2 Will the third party have access to any special categories of data? This includes information relating to health, racial or ethnic origin, religious or political beliefs, trade union membership, genetic data, biometric data or information relating to a person's sex life or sexual orientation.

4.3.3 Will the third party be carrying out any monitoring of individuals (e.g. through use of CCTV)?

4.3.4 Will the third party be making any wholly automated decisions (decisions made by automated means without any human intervention) about individuals using their personal data?

4.3.5 Will the third party be carrying out any processing that an individual may consider particularly intrusive or sensitive?

4.4 If the answer to any of the questions above is "YES" then the processing is not low risk and you will need to consider which optional questions should be included in the DD Questionnaire. Even if none of the questions above have been answered "YES" it may still be the case that it is appropriate to use some of the optional questions. The Purchasing Department will consider the nature of the personal data being handled by the third party and the potential impact on the individual if there is any breach of data protection requirements when considering which questions to include.

4.5 Following the determination of the inclusion of "optional questions", the Purchasing Department should delete the column in the DD Questionnaire which contains internal guidance information.

5 **Future actions**

5.1 If you decide that you are required to carry out due diligence on the supplier, you should make sure that due diligence is also conducted at frequent future intervals to explore whether (i) the nature of the supplier's data processing and the contract between Elior and the supplier has changed, and (ii) the adequacy of the supplier's compliance with its data protection obligations in the contract. You should always document such due diligence for a regulator's future inspection.

**Appendix 2**

**Annex A**

**Elior Supplier Due Diligence Questions**

| Question no. | Self-certification data protection questions | | Is this a required or optional question? [Drafting note: This entire column must be deleted before circulating with the supplier] |
|---|---|---|---|
| **1** | Please certify whether you have all necessary measures in place to ensure compliance with applicable data protection legislation (including UK GDPR). If the answer to this question 1 is yes, please ignore question 2. | Yes ☐<br>No ☐ | **Required** – indication of compliance with UK GDPR requirements. |
| **2** | If not, please provide a detailed explanation as to when you expect to be in a position to comply with the UK GDPR requirements. | Yes ☐<br>No ☐ | **Required** – indication of compliance with UK GDPR requirements. |
| | | | |
| **3** | **Processing details**<br><br>Please complete the table attached at Appendix 2, Annex B to describe the data processing activities that will be undertaken. | | **Required** to enable contract to be populated. |
| **4** | **Accountability**<br><br>Please provide evidence of the measures that you have in place to ensure compliance with applicable data protection legislation. This should include evidence of the following:<br><br>***Governance***<br><br>• How you will comply with your governance obligations under the UK GDPR, including information about who has responsibility for ensuring data protection compliance. Please include contact details of the Data Protection Officer (or, if you consider that a Data Protection Officer is not required, the reasons for this conclusion and the contact details of the individual responsible for data protection compliance) and details of the board member or senior manager with responsibility for data protection compliance. | | **Required** – evidence of compliance with UK GDPR requirements. |

## Data Protection and Privacy Policy

| | | |
|---|---|---|
| | ***Policies and procedures***<br>• Documented policies and procedures relating to data protection compliance.<br>• How you ensure that data protection requirements set out in policies are implemented and complied with. | |
| | ***Training***<br>• Data protection and security training provided to all personnel handling personal data (**Training**) including details of how (i) often the Training is reviewed for accuracy; (ii) often the Training is undertaken; and (iii) how completion of the Training is documented and monitored. | |
| | ***Records***<br>• How you maintain records of data processing activities as required under the UK GDPR. | |
| **5** | **Technical and organisational measures ("TOMs")**<br>Please provide evidence of the TOMs that you have in place to protect against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Please include (without limitation) details of the measures you have in place to ensure compliance with UK GDPR which should include the following, or, an explanation of why these measures are not relevant:<br>• Pseudonymisation and encryption of personal data<br>• Ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services<br>• Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident<br>• Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing. | **Required** – evidence of compliance with UK GDPR requirements. |
| **6** | **Individuals' rights**<br>Please provide evidence of the procedures/measures you have (or will have) in place to enable compliance with individuals' rights under data protection legislation. Please include (without limitation) details of how you will assist Elior in ensuring compliance with the following rights | **Required** – evidence of compliance with UK GDPR requirements. |

## Data Protection and Privacy Policy

| | | |
|---|---|---|
| | within statutory timeframes or an explanation of why this is not relevant for your organisation:<br>• Provision of privacy notices to individuals to meet transparency requirements under the UK GDPR<br>• Right of access to personal data by data subjects<br>• Right to rectify inaccurate personal data without undue delay<br>• Right to delete personal data under the UK GDPR<br>• Right to restrict processing of personal data under the UK GDPR<br>• Right to data portability under the UK GDPR<br>• Right to object to marketing and profiling<br>• Right not to be subject to automated decision-making | |
| **7** | **Data protection by design and default**<br><br>Please provide evidence of the measures you have in place to ensure compliance with the data protection by design and default requirements in the UK GDPR. This should include (without limitation):<br>• details of how you minimise the personal data that is collected and processed;<br>• details of how access to personal data is minimised only to those who need to see personal data; and<br>• details of how pseudonymisation is used where appropriate. | **Required** – evidence of compliance with UK GDPR requirements. |
| **8** | **Joint controllers**<br><br>If you consider that there will be activities in relation to which you and Elior will jointly determine the purposes and means of data processing, please outline these activities and the proposed allocation of responsibilities between Elior and the service provider for data protection compliance. | **Required** – to enable contract to be populated. |
| **9** | **Information and Assistance**<br><br>Please provide evidence of the measures and procedures you have in place to provide information and assistance to Elior as necessary to enable and demonstrate compliance with applicable data protection legislation.<br><br>Please include (without limitation) an explanation of how | **Required** – evidence of compliance with UK GDPR requirements. |

| | | |
|---|---|---|
| | you will assist Elior in ensuring compliance with UK GDPR. | |
| **10** | **Breach notification**<br><br>Please provide details of how you will comply with the UK GDPR's breach notification requirements and in particular, how you will notify Elior of any personal data breaches. | **Required** – evidence of compliance with UK GDPR requirements. |
| **11** | **Personnel**<br><br>Please provide details of vetting procedures carried out in relation to personnel who will have access to personal data. | **Optional** - consider including if particularly sensitive information will be processed by the third party. |
| **12** | **Sub-contractors**<br><br>Please provide details of how you will comply with the requirements of the UK GDPR in relation to the appointment of sub-contractors which should include, information about the steps taken to carry out due diligence in relation to data protection measures that sub-contractors have in place and how on-going compliance with such measures is monitored. | **Optional** - consider including if sub-contractors are being used by the third party and sub-contractors will be processing personal data. |
| **13** | **Complaints, claims or regulatory investigations**<br><br>Please provide details of any data protection complaints, claims or regulatory investigations to which you have been subject, including (without limitation):<br><br>• details of the nature of complaints/breaches;<br><br>• whether issues have been resolved; and<br><br>• the outcome of any regulatory investigations. | **Optional -** consider inclusion for higher risk projects where the third party will have access to large volumes of data or particularly sensitive/risky data. |

## Data Protection and Privacy Policy

**Appendix 2**

**Annex B**

**Supplier processing details**

| | | | |
|---|---|---|---|
| **Categories of data** | *[Supplier to insert details of the categories of Personal Data that it will process]* | | |
| **Categories of Data Subjects** | *[Supplier to insert details of the categories of data subjects whose Personal Data will be processed]* | | |
| **Processing Operations** | *[Supplier to insert details of all processing activities it will conduct]* | | |
| **Location of Processing Operations** | *[Supplier to insert details of all locations where the personal data will be processed]* | | |
| **Identity of sub-contractors** | ***Sub-contractor's name, registration number, registered office address and the service provided*** | ***Location of sub-contractor's processing operations*** | |
| | *[Supplier to insert details of all sub-contractors, including full legal name registered address and a description of the processing operations undertaken by each sub-contractor]* | *[Supplier to insert details of locations where Personal Data will be processed by each sub-contractor]* | |
| **Transfer outside the EEA** | ***Supplier or subcontractor's name*** | ***Location of processing operations*** | ***Adequacy mechanism relied on*** |
| | *[Supplier to complete if it or its sub-contractors are processing personal data outside the EEA]* | *[Supplier to specify location of third party or relevant sub-contractor processing]* | *[Supplier to specify the adequacy mechanism relied upon to ensure the transfer of the personal data is lawful.]* |
| **Purposes** | *[Supplier to insert details of all purposes for which it will process the Personal Data]* | | |

# Data Protection and Privacy Policy

**Appendix 3**

**Subject Access Requests Policy**

## Scope

A request by an individual to exercise this right is called a subject access request (**SAR**).

This Policy applies to all of our colleagues (including colleagues and contractors) and sets out:

- How individuals can make a SAR;
- What our obligations are under a SAR; and
- How to recognise a SAR and the steps that you should take if you receive a SAR.

## Definitions

Some of the terms used in this Policy have very specific meanings. These include:

- **data controller**: this means the entity which determines how, and for what purposes, personal data will be collected and used, and which is responsible for complying with data protection legislation. Elior is a data controller in relation to personal data we process about customers, colleagues, suppliers, consumers and contractors;
- **data processor**: this means an organisation which processes personal data on behalf of Elior. Elior is responsible for each data processor's use of personal data;
- **data subject**: this means the individual to whom personal data relates;
- **personal data**: (or personal information): this means any information about a living individual (including customers, colleagues, suppliers, consumers and contractors of Elior) who can be identified from that information, or from that information together with other information held by Elior. Personal data may include things like completed medical diet request forms; colleague files; and correspondence with a consumer;
- **processing**: this means obtaining, recording, organising, retrieving, using, disclosing and simply holding information.

## Responsibilities

If we receive a SAR, we are under a statutory obligation to conduct a reasonable and proportionate search of all our electronic systems and any structured hard copy files to locate personal data concerning that data subject.

We are then obliged to:

- inform the data subject whether we are the data controller of any personal data about that data subject. This means that even if we do not hold any personal data about the individual, we need to tell him/her that this is the case;
- provide a copy of the relevant personal data to the data subject;
- if it is not obvious from the copy of the personal data, tell the data subject:
    - the source of the data;
    - what the personal data constitutes;
    - the purposes for which the personal data is processed;
    - the types of third parties to whom the personal data may have been disclosed;
    - how long we envisage the personal data will be stored for;
    - the fact that the data subject has the right to request that we correct, delete or restrict processing of his or her personal data;
    - whether we make any wholly automated decisions about the data subject based on that personal data; and
    - the fact that the data subject has the right to complain to the Information Commissioner's Office about our processing of his or her personal data.

## Data Protection and Privacy Policy

We must respond to these subject access requests and provide the information listed above (which can take some time collating documents and taking comments from the business) as soon as possible and in any event **within one month**.

**Receiving and recognising SARs**

It is very important that all of our colleagues are aware of how to recognise a SAR so that we can comply with our obligations under the legislation.

A SAR is any written request by an individual to see his or her personal data. There is no requirement for a SAR to be in a particular format, nor for it to be sent to any particular person within an organisation. A SAR will be valid as long as it is in writing and sent to any colleague.

A SAR does not have to state that it is a SAR, reference any data protection legislation or even refer to "personal data" in order to be valid.

If you are concerned that you may have received a SAR or have received one, please contact your HR Business Partner immediately providing a copy of the request. Colleagues must cooperate with the HR Business Partner in collating responses to subject access requests.

**What can we ask for?**

We are entitled to ask for certain information from the data subject in order to enable us to respond to that individual's SAR:

- We are entitled to ask for sufficient identification to enable us to confirm the data subject's identity. We may require a certified copy of the individual's photographic ID (such as a passport or driving licence). However, in certain circumstances we may require further identification, for example if:
    - a SAR is being made by a third party on behalf of the data subject;
    - the SAR is made by someone whose name or details we do not recognise; or
    - contact details provided in the SAR do not match the contact details we hold on file for the data subject.
- We are also entitled to ask for any further information that we reasonably require to enable us to locate the personal data that is being requested. For example, if it is not clear from the individual's request what information he or she is requesting, we can ask for clarification. Although this may help us to focus our searches, we cannot force the individual to narrow the scope of his or her SAR.

The one month statutory period does not start to run until we have received the information above.

As long as a SAR is in writing, we cannot require it to be made in a particular form or format. This does not mean that we cannot ask an individual to fill out a form to provide further information; however if the individual refuses to fill out the form and we are able to locate the data requested without any further information, we cannot refuse to comply with the request on the basis that the form has not been completed.

In the HR Ways Guide to Data Protection you will find a sample initial response letter to a SAR request letter. Please seek advice from your HR Business Partner if you feel that you need to amend this letter in any way, your HR Business Partner should always be informed of the Subject Access Request and oversee the process with you.

**Third Party SARs**

Sometimes data subjects will ask a third party, such as a solicitor, family member or friend, to make a SAR on their behalf. There are certain steps that we should take to make sure that we can disclose the relevant information to the third party.

## Data Protection and Privacy Policy

- We may need to request further identification documents from the individual in this situation to ensure that we are confident that the individual requesting the third party to act on his/her behalf is the data subject.
- We will need to make sure we have a document authorising us to send the data subject's personal data to the third party, for example a power of attorney or letter of authority. We may also require this if two or more data subjects make a joint SAR.

**What information do we have to provide?**

Data subjects are entitled to see a copy of their personal data. This does not mean that we have to send them a full copy of every document that contains their personal data.

We are entitled to withhold, or redact, certain information from documents containing personal data, including:

- information which is not "personal data" (for example, a comment in an email about the weather);
- third party personal data (for example, names of other colleagues). We can provide third party data where the third party has consented or it is reasonable to disclose that data (for example, if the information is in an email that the data subject has already seen);
- information that is legally privileged (for example, correspondence between us and our solicitors for the purposes of taking legal advice);
- information that is used for the purposes of management planning and forecasting (for example, information about a proposed re-organisation which might result in making the data subject redundant);
- information that is processed for the purposes of preventing or detecting crime (for example, internal emails discussing a potentially fraudulent individual); and
- in the case of a current or former colleague, confidential references that we have given to other organisations (though note that we must provide the personal data contained within references that we have received).

**Call recordings and CCTV**

Individuals may also request copies of recordings of calls to which they have been a party, or copies of CCTV footage of them that we hold.

If call recordings/CCTV footage exist, we may also be obliged to disclose the personal data contained in those recordings/footage, except where we would not be able to do so without disclosing personal data of third parties who have not consented to the disclosure of their data and where it would not be reasonable to disclose that data.

We may be able to disclose transcripts of call recordings or certain clips of CCTV footage. Please let your HR Business Partner know if a data subject has requested call recordings and/or CCTV footage.

**What to do if you receive a SAR**

All colleagues who receive SARs for data relating to individuals must forward these **immediately** to your HR Business Partner together with any information that you know about the background to the SAR.

If you receive a telephone request for information about an individual, you should:

- take steps to verify the individual's identity on the phone and not disclose any personal data about the individual unless you are sure of the caller's identity;
- ask the caller to put the request in writing if you are not sure of the caller's identity and/or the caller is looking to make a formal SAR; and
- refer the call to your HR Business Partner if you are not sure how to deal with the request.

## Data Protection and Privacy Policy

### Making a SAR

If you would like to make a SAR, please send your written request to the HR Service Desk.

# Data Protection and Privacy Policy

## Appendix 4

## Individuals' Rights Policy

**1** What rights do individuals have under data protection legislation?

1.1 Under the General Data Protection Regulation (**UK GDPR**) individuals have the following rights:

1.1.1 the right to be informed;

1.1.2 the right of access;

1.1.3 the right to rectification;

1.1.4 the right to erase;

1.1.5 the right to restrict processing;

1.1.6 the right to data portability;

1.1.7 the right to object;

1.1.8 rights in relation to automated decision making.

1.2 The sections below provide a detailed explanation of what each of these rights involves so that all colleagues are able to recognise these rights if an individual seeks to exercise them. The Policy also explains the timeframes for responding to requests and the consequences if we fail to respond as we should. The right of access in 1.1.2 above is dealt with in Appendix 3, Subject Access Request Policy.

### 2 The right to be informed

2.1 Individuals have a right to be informed about how Elior will use and share their personal data. This explanation must be provided to individuals in a concise, transparent, intelligible and easily accessible format. Privacy notices must be written in clear and plain language and must be provided free of charge.

2.2 We must ensure that we provide privacy notices to individuals at the point where we collect data from them if we are collecting data directly. If we obtain data from a third party then the information must be provided to individuals within one month or, if earlier, at the point of first contact with the individual or before data is disclosed to a third party.

2.3 The UK GDPR sets out a list of specified information that must be provided to individuals in privacy notices. We must therefore ensure that all privacy notices contain this mandatory information.

2.4 We satisfy this requirement by ensuring that appropriate privacy notices are included at all data collection points.

### 3 Right to rectification

3.1 Individuals have a right to have any inaccurate or incomplete personal data rectified.

3.2 If we have disclosed the relevant information to any third parties we are also responsible for taking reasonable steps to inform those third parties of the rectification where possible.

3.3 If we dispute that the information is inaccurate then it will be necessary to go back to the individual and explain why the information is not being rectified. Individuals should also be informed at this point that

they have a right to complain to the Information Commissioner's Office if they do not agree with this decision.

3.4 If you receive a rectification request you should follow the following procedure:

3.4.1 Verify the accuracy of the individual's personal data;

3.4.2 Verify the individual's identification documents in accordance with section 10; and

3.4.3 Update the records of the relevant individual.

3.5 Should you be unable to complete any of the steps listed above or have any additional concerns, advice should be sought from your HR Business Partner.

## 4 Right to erasure

4.1 Individuals have a right to request that certain information we hold is erased. This is also known as the "right to be forgotten". This is not a blanket right to require all personal data to be deleted. Rather, the right will be triggered in the following circumstances:

4.1.1 If we are continuing to process personal data beyond the period when it is necessary to do so for the purpose for which it was originally collected.

4.1.2 If we are relying on consent as the legal basis for processing and the individual withdraws their consent

4.1.3 If we are relying on legitimate interest as the legal basis for processing and the individual objects to this processing and there is no overriding compelling ground which enables us to continue with the processing.

4.1.4 If the personal data has been processed unlawfully (i.e. in breach of the requirements of the UK GDPR).

4.1.5 If it is necessary to delete the personal data to comply with a legal obligation.

4.2 There are some exemptions to the right to erasure so even if one of the triggers above is met it may not be necessary to erase the relevant information. If information is required to exercise or defend legal claims then it is not necessary to delete the data. We are also permitted to retain personal data where there is a public interest task which requires the data to continue to be processed or for research purposes.

4.3 If you receive a request to erase personal data advice should be sought from your HR Business Partner.

## 5 Right to restrict processing

5.1 Individuals have a right to block the processing of their personal data in certain circumstances. This right arises in the following circumstances:

5.1.1 If an individual disputes the accuracy of personal data then processing of that data should be restricted whilst we are verifying the accuracy of the personal data.

5.1.2 If an individual has raised an objection to processing then processing should be restricted while we consider whether the objection should be upheld.

5.1.3 If processing of personal data is unlawful and the individual opposes erasure and requests restriction instead.

5.1.4 If the personal data is no longer required but the individual requires the data to be retained to establish, exercise or defend a legal claim.

5.2 If a request to restrict processing is made then it will be necessary for us to determine whether the request should be upheld and whether procedures need to be put in place to restrict use of the relevant data. If the request to restrict processing is not upheld then the individual needs to be notified of the reasons for this.

5.3 If you receive a request to restrict processing, advice should be sought from the respective Head of Function.

## 6 Right to data portability

6.1 In certain circumstances individuals can request to receive a copy of their personal information in a commonly used electronic format. This right only applies to information that individuals have provided to us (for example by completing a form or providing information through a website). In addition, if information about an individual has been gathered by monitoring their behaviour then this information will also be subject to the right to data portability. However, any analysis done by us in relation to an individual would not constitute information that they have provided to us and therefore is not subject to the right of data portability.

6.2 The right to data portability only applies if the processing that we are carrying out is based on the individual's consent or if the information must be processed for the performance of a contract. In addition, the right only applies in relation to data processing that is carried out by automated means (i.e. electronically).

6.3 In order to provide the data in response to a portability request the data must be provided in a commonly used and machine readable form.

6.4 The individual also has a right to request that the data is transferred directly to another organisation. If this is technically feasible then we must comply with such a request.

6.5 If you are processing data based on individual's consent or if the information must be processed for the performance of a contract and you receive a data portability request advice should be sought from the respective Head of Function.

## 7 Right to object

7.1 Individuals have a right to object to data processing being carried out by us in the following circumstances:

7.1.1 If we are processing data (including for profiling purposes) based on legitimate interests or for the performance of a task in the public interest.

7.1.2 If we are using personal data for direct marketing purposes.

7.1.3 If information is being processed for scientific or historical research or statistical purposes.

7.2 If an objection is raised in relation to data that is being processed on a legitimate interest or public interest ground then a balancing test must be carried out to consider whether there are any compelling legitimate grounds which enable us to continue processing the data. In each case the outcome of this decision and the reasons for it must be documented.

7.3 If an objection is raised in relation to direct marketing then the objection must be upheld and no balancing test will be carried out.

7.4 Individuals must be informed that they have a right to object at the point of data collection and the right to object must be explicitly brought to the attention of the individual and be presented clearly and separately from any other information.

7.5 If you receive an objection to marketing you must ensure that the relevant individual is flagged as an "opt-out" on all relevant databases immediately. If an objection is raised in relation to data that is being processed on a legitimate interest or public interest and you receive an objection to other data processing activities advice should be sought from the Marketing Department.

## 8 Time frames for responding to requests

8.1 In relation to the right to be informed, information must be provided at the point of data collection where information is collected directly from an individual. Where information is collected from a third party then information must be provided within one month at the latest

8.2 In relation to all other rights we must respond without undue delay and in any event within one month. In exceptional cases this one month period may be extended by two further months if the request is particularly complex and involves a large number of requests. If we wish to make use of this extension then the individual must be informed within the initial one month period and the reasons for the delay must be explained. The ability to extend the one month period is only likely to arise in exceptional cases. If you wish to extend the period for responding to a request you must consult with the respective Head of Function.

## 9 Verification of identity prior to taking any action in relation to a request

9.1 We must be satisfied that the individual making the request is in fact the individual about whom the information relates. If we have an ongoing relationship with the individual and have no reason to doubt the validity of a request then there is no need to take further steps. For example, if an colleague makes a request using their known employment email address then no further steps to verify identity would be required. However, if a consumer made a request and asked for information to be sent to an address that was not known to us then additional steps should be taken to verify the identity of the individuals.

## 10 Can we charge a fee?

10.1 In most cases it is not possible for us to charge a fee to comply with requests made by individuals. However, if any request is manifestly unfounded or excessive, in particular it is a repeat request, then we may charge a reasonable fee taking into account the administrative costs of providing the information or taking the action required. Alternatively in these circumstances we may refuse to act on the request. In each case we will have to be able to demonstrate that the request is manifestly unfounded or excessive and must document the reasons for this decision. This exemption may only be relied on in exceptional circumstances and if you wish to refuse a request on these grounds the decision should be escalated to the respective Head of Function to be authorised.

## 11 What happens if we fail to comply with a request?

11.1 Failure to comply with individuals' requests under the UK GDPR are considered to be serious breaches of an individual's rights. Such breaches can attract the maximum possible fine under the UK GDPR regime, which equates to up to a 4% of Elior Group turnover or €20million. Failure to comply could also have an adverse effect on the individual. It is therefore important that all requests are recognised and are acted on promptly to enable Elior to respond to requests correctly and within the one month time frame.

# Data Protection and Privacy Policy

## Appendix 5

## Breach Management Policy

### 1 Introduction

1.1 If a data security breach occurs this can have serious implications for us and any individuals whose Personal Data (as defined in Appendix 3) may have been lost or accessed in an unauthorised manner.

1.2 This Breach Management Policy explains the procedure that you should follow as soon as you become aware of a data security breach.

1.3 This Policy will help us ensure that the consequences of data security breaches are managed as quickly and effectively as possible and ensure compliance with our legal obligations, which may involve reporting data security breaches to the Information Commissioner and/or to affected individuals.

1.4 This Policy sets out the procedure with which all colleagues and contractors (referred to in the remainder of this Policy collectively as **colleagues**) must comply if they become aware of a data security breach.

### 2 What is a data security breach?

2.1 A data security breach occurs if there is breach of security that leads to:

2.1.1 the accidental or unlawful destruction, loss or alteration of Personal Data; or

2.1.2 any unauthorised disclosure of or access to Personal Data.

2.2 Examples of data security breaches include:

2.2.1 Loss or theft of data or equipment on which Personal Data is stored;

2.2.2 Inappropriate access controls allowing unauthorised use;

2.2.3 Equipment or technical failure leading to loss of or corruption of data;

2.2.4 Human error, for example sending an email to an incorrect recipient or forgetting to use the 'BCC' field instead of the 'CC' field;

2.2.5 Sending an excel spreadsheet containing personal data to the wrong recipient;

2.2.6 Hacking attack; or

2.2.7 "Blagging" offences where information is obtained by deceiving the organisation who holds it into believing the person requesting the information is entitled to access the information.

2.3 A personal data breach can have serious consequences for the individuals concerned such as identity theft and fraud and it is important that each and every one of us takes responsibility for any potential, suspected, threatened or actual security breaches.

### 3 What do you do if there is a data security breach?

3.1 You must contact the recipient of the information immediately and let them know it was sent in error, ask them to delete the email and confirm in writing back to you that they have done so, without sharing the information further. You must also report **immediately** any potential, suspected, threatened or

actual security breach to the Legal Department by contacting the Legal Department. We only have 24 hours to report the most serious of breaches, and therefore why you must report a potential breach immediately. The Legal Department will ascertain the nature and severity of the breach and will manage the breach in accordance with this Policy.

3.2 Your notification should include the following details:

3.2.1 Your name, job title and telephone and email contact details;

3.2.2 Description of what has happened, with confirmation that you have asked the recipient to delete the information and confirmation has been received from such recipient that this has been done, without them having shared the information further;

3.2.3 Volume of data involved and number of individuals affected;

3.2.4 Type(s) of data involved, including personal data and which individuals this affects;

3.2.5 Status of security breach (i) potential (ii) suspected (iii) threatened (iv) actual (and if actual, has this been isolated (and how) or is it ongoing?);

3.2.6 Who is aware of the breach;

3.2.7 What actions have been taken to address the breach and have these mitigated any adverse effects; and

3.2.8 Any other relevant information.

**4 Breach management procedure**

4.1 The Legal Department will be responsible for co-ordinating the response to data security breaches.

4.2 The Legal Department shall:

4.2.1 Investigate the reported breach to establish the scale and nature of the breach;

4.2.2 Consider what can be done to recover any loss of Personal Data;

4.2.3 Identify the safeguards in place, or to be put in place, to protect against any misuse of the Personal Data;

4.2.4 Identify any relevant departments to assist and if appropriate, any third parties, such as banks, websites, insurers, police or credit card companies to prevent fraudulent use of Personal Data;

4.2.5 By establishing the cause, determine whether any further actions can be taken to contain the breach e.g. taking systems offline, changing access codes, finding lost equipment etc;

4.2.6 Determine the value of the Personal Data to any third party in receipt; and

4.2.7 Take all necessary steps to mitigate the effects of the data breach.

4.3 The Legal Department will act as a contact point for the business and the affected individuals and lead the co-ordination of remedial action.

# Data Protection and Privacy Policy

## 5 Breach reporting

5.1 In some circumstances it will be necessary to report data security breaches involving Personal Data to the Information Commissioner. It may also be necessary to notify individuals of a data security breach if the information is particularly sensitive or if individuals need to take steps to protect themselves against potential misuse of their Personal Data.

5.2 The Legal Department shall be responsible for determining whether a data security breach needs to be reported to the Information Commissioner and whether affected individuals need to be notified.

5.3 In order to evaluate whether a data security breach needs to be reported to the Information Commissioner or whether individuals need to be notified of the breach, the Legal Department shall take account of all relevant regulatory guidance and shall evaluate the likely risk to individuals. When carrying out this evaluation the Legal Department shall consider whether there are any risks of:

5.3.1 Identity theft or fraud;

5.3.2 Financial loss;

5.3.3 Reputation damage; or

5.3.4 Any significant economic or social disadvantage to the individual(s) concerned.

5.4 If a data security breach involves Personal Data that is being processed by Elior on behalf of a third party, details of the data security breach may need to be notified to that third party. The Legal Department shall be responsible for determining which data security breaches need to be notified to third parties.

## 6 Post breach review

6.1 Following a data security breach, the Legal Department and, if appropriate, the UK GDPR Governance Committee shall evaluate the data security breach and the response to the breach and shall prepare a report for the Leadership Team. The report shall:

6.1.1 Summarise the data security breach event;

6.1.2 Outline the steps taken in accordance with this Policy;

6.1.3 Describe the effects of the Data Security breach;

6.1.4 Detail the measures taken by the business to prevent similar breaches happening again; and

6.1.5 Set out recommendations for any additional preventative steps that can be taken, including measures to improve the breach management response.

## 7 Data security breach log

7.1 The Legal Department shall record details of all reported data security breaches in a data security breach log.

# Data Protection and Privacy Policy

## Appendix 6

## Data Retention Policy

### 1 Introduction

1.1 This Policy provides guidance on appropriate retention periods for different categories of records and on the standards with which all colleagues and contractors must comply when creating, storing and disposing of records.

1.2 This Policy applies to all records, whether in paper or electronic form, that are created, received or handled by colleagues during the performance of their duties. It also applies to records held in audio or visual form such as call recordings and CCTV footage.

### 2 Creation and maintenance of records

2.1 All records must remain complete and intact, including all emails, contemporaneous notes of conversations, dates and telephone messages, so that they can be relied on in case of complaint or litigation.

2.2 Records must be kept and stored securely so that they cannot be accessed by unauthorised third parties.

2.3 We have to make sure that information held within records is kept up-to-date. You should therefore monitor records that you are in charge of on a regular basis and consider whether any updates need to be made to those records. For example, if you are in charge of personnel files, you should make sure that relevant staff check their contact details from time to time and update them if necessary.

### 3 Retention of records

3.1 We must retain some records for set periods of time and also have obligations to delete certain information when it is no longer needed. The table in Annex 1 to this Appendix 6 to this document sets out the retention periods for which records must be kept.

3.2 You must ensure that all records are retained in line with the periods set out in Annex 1 and are deleted at the end of the relevant period in accordance with section 4 below.

3.3 In some cases there may be a good reason to keep records for a longer period (for example if there is an ongoing legal claim).

### 4 Disposal of records

4.1 You must make sure that when records are deleted in line with Annex 1, they are deleted securely so that they cannot be accessed by a third party once we have disposed of them.

4.2 For example, hardcopy records should be shredded or placed in our confidential waste bins. Documents held electronically should be deleted in their entirety from our systems. Please speak to the IT Team to establish how these documents can be fully deleted.

4.3 If you need to dispose of equipment which might contain personal data, for example computers, hard drives or other hardware, you must make sure that equipment is wiped prior to disposal. This means that all personal data held on that piece of equipment must be erased thoroughly from the equipment. Please speak to the IT Team to establish the best way to wipe equipment.

# Data Protection and Privacy Policy

## Annex 1

## Retention Periods

| Type of Record | Retention Period | Reason for Retention |
|---|---|---|
| **HR Documents** | | |
| Employee Personnel file | 6 years from end of employment | For the provision of references and in case of claims by employees |
| Application Forms - unsuccessful candidates | 12 months from application date | To enable contact to be made if other opportunities become available. |
| **Financial Documents** | | |
| Till audit rolls<br>inSIGHT reports<br>Cash received Analysis<br>sales Invoices<br>Supplier order book / forms<br>Production & Wastage records | 3 months | To enable auditing and query resolution |
| Site specific financial records e.g. cost of sales<br>Completed Bank Books | 1 year | To enable auditing and query resolution |
| Till Z readings<br>Cash carried Forward Analysis<br>Bank slips<br>G4S collection slips<br>PDQ End of Day reports<br>PDQ advice slips<br>ATM Daily Close reports<br>Non-electronic Invoices<br>Cash purchase receipts<br>Transfer slips and Function & Event, hospitality & free issue records<br>Booking forms / quotes and/or client communications<br>Stock sheets (N/A if using inSIGHT)<br>Colleague timesheets / signing in & out records | 6 years | To enable auditing and compliance checks |
| **Safety & Wellbeing Documents** | | |
| Food allergens report<br>Cooking Temperature records CD4, 5 & 6<br>Probe calibration records CD9 & 21<br>Delivery records CD2 & 2a<br>Fridge/freezer temperature records CD3 & 3a<br>Service temperature records CD8<br>Cooling records CD7<br>Pest control records CD12 & 12a<br>Food complaint and related records CD14,15,16 & 17 | 1 year | To enable auditing and compliance checks |
| Responsibilities records sheets - Food Safety and health & safety<br>Monthly internal audit records SR2 / CD18<br>Monthly H&S meeting minutes SR1<br>Repair requisition forms SR3 & CD10<br>Catering vehicle records SR16, 17 & 18<br>Temporary staff & Contractor checks SR7, 8 & 9<br>Opening & Closing checklist SR22<br>Training records SR4a, 4b, 4c & CD19<br>Food Safety certificates L2 & 3<br>Cleaning schedules CD10 & 11<br>Training Matrix SR5a, b & CD22<br>Hygiene Audits (EHO / S+W)<br>COSHH risk assessments including chemical ID record SR19<br>Risk assessments RA001 - 114 and site specific SR10, 11a, 11b, 12, 13, 14 & 15<br>Night worker health assessments SR21 | 3 years & 4 months | To enable auditing and compliance checks |

# Data Protection and Privacy Policy

## Appendix 7

## Strong Password Policy

### 1 Introduction and background

1.1 We handle a large amount of personal data and other confidential and commercially sensitive information about the Company itself, our clients, colleagues, consumers, contacts, suppliers and other individuals or businesses.

1.2 We have obligations under data protection laws to ensure that adequate security measures are in place to protect personal data. It can also be very damaging to our business if personal data or other confidential or commercially sensitive information is put at risk.

1.3 One of the ways in which this kind of information can be put at risk is through our systems being accessed by unauthorised third parties. It is therefore vital that access to our systems is controlled, protected and only given to authorised colleagues and contractors.

1.4 Part of ensuring that our systems are secure and cannot be accessed by unauthorised third parties is by making sure that all Colleagues and contractors use passwords that are strong, secure and cannot be guessed, deduced or accessed by anyone else.

### 2 Scope of this Policy

2.1 This Policy applies to all colleagues and contractors and sets out the requirements with which you must make sure the password you use to access our systems is sufficiently strong to make sure our information is protected.

### 3 Strong password requirements

3.1 When you choose a password to access our systems, you must make sure that your password:

3.1.1 is at least seven characters long;

3.1.2 is changed at least every 42 days. You will receive a reminder to change your password 5 days before your current password is due to expire and then at regular intervals until your current password expires; and

3.1.3 is not the same as any of your previous five passwords.

3.2 If your password does not comply with the requirements above, you will not be able to set it and you must choose a new password. We do also recommend that your password contains at least one upper case letter, at least one lower case letter, at least one number and at least one "special character" (e.g. @, %, £, *, !, ?);

3.3 If you need to reset your network password you should use the secure Password Reset Tool provided by the IT Department.

3.3.1 You will need to register your details on the password reset tool before you are able to use it. To do this, you will need to input your current user name and password credentials and provide answers to different security questions relating to your personal information (e.g. mother's maiden name, name of first school attended, name of first pet).

3.3.2 When you need to reset your password by using this tool, you will be asked to confirm the answers you provided to these questions.

3.3.3 You should protect the answers to these questions in the same way that you protect your password as detailed in Item 4 within this Appendix.

3.3.4 If you have any queries about the tool (including how to access, registering your details and resetting your password) please contact the IT Service Desk for advice and assistance.

3.4 You should also make sure that any password you use:

3.4.1 does not contain any word that is spelled completely and correctly in plain letters;

3.4.2 is not the same as any password that you use to access any other systems or accounts, such as your personal email or social media accounts. Some Elior systems are classed as single sign-on and use the same network password (e.g. logon to computer on Elior network, email access, Extranet). You should use different passwords for Elior systems which do not use a single sign-on account (e.g. inSIGHT, MyView, StarChef);

3.4.3 does not contain any information about you, for example your date of birth or name. This makes your password very easy to guess;

3.4.4 does not include any other information that someone would find it easy to guess, for example a family member's or pet's name or details; and

3.4.5 is easy for you to remember. The strongest passwords are very long, random combinations of letters, numbers and characters, but these may be hard to remember.

3.5 A good approach when considering your password is to:

3.5.1 think of a random sentence or word which is not directly related to you;

3.5.2 replace some of the letters with numbers and special characters; and

3.5.3 finally, capitalise some of the remaining letters.

Some examples of strong passwords which take this approach are set out below.

## 4 Protecting your password

4.1 You must take the following steps to protect your password and make sure no one else finds out what it is:

4.1.1 never write your password down; and

4.1.2 never share your password with anyone else, even with another Elior colleague or a close friend or family member.

## 5 What to do if you think someone knows your password

5.1 If you think that someone knows your password, you must:

5.1.1 immediately change your password to a new password which complies with the requirements of this Policy;

5.1.2 immediately inform your line manager that the password may have been jeopardised; and

5.1.3 if you believe that the release of your password may have put personal data at risk, take the steps set out in our Data Breach Management Policy. Please see our Legal Sub Policy: Data Protection and Privacy for more information about what constitutes "personal data".

## 6 Examples of strong passwords

6.1 Some examples of strong passwords are the following:

6.1.1 iL!k3c@T5

6.1.2 j3lLi22fi$H

6.1.3 d3lT@gAm*4

6.1.4 dR/s3u55#

6.1.5 p4r!sI5gr3@T

6.2 Examples of password which are not strong and do not comply with this policy are as follows:

6.2.1 Pa55w0rd!

6.2.2 Mike1975

6.2.3 abc123ABC

6.2.4 ilovedogs

6.2.5 qwerty987

## 7 Questions and concerns

7.1 If you have any questions or concerns about this Policy, please contact the Legal Department.

# Data Protection and Privacy Policy

## Appendix 8

## Data Protection Impact Assessment Policy

### 1 Introduction

1.1 This Data Protection Impact Assessment Policy explains our policy on carrying out Data Protection Impact Assessments (**DPIAs**) and applies to all colleagues and contractors.

1.1 This Policy will help the Legal Department ensure that DPIAs are carried out as efficiently and effectively as possible and ensure compliance with our legal obligations.

### 2 What is a DPIA?

2.1 A DPIA is an assessment of the impact of proposed processing on the protection of personal data. This enables us to ensure that privacy risks are identified at the outset and that appropriate measures are taken to mitigate those risks. This, in turn, assists in ensuring compliance with regulatory obligations in relation to personal data and that the impact on individuals of our data processing is proportionate and justified.

2.2 Failure to undertake a DPIA where one is required and to implement the outcomes of the same could have serious consequences for us including the imposition of significant fines.

### 3 When is a DPIA required and when must it be undertaken?

3.1 For projects involving a large amount of personal data or where personal data is being used in a new or more intrusive way, it is necessary to carry out a thorough assessment of privacy risks before implementing the project.

3.2 For certain types of projects it is also a legal requirement to carry out a DPIA. This is the case where the data processing poses a high risk to the rights of individuals. This will include (without limitation) the following types of data processing activities:

3.2.1 Where we are processing a large volume of special categories of data. Special categories of data include the following information:

(a) racial or ethnic origin

(b) political opinions

(c) religious or philosophical beliefs

(d) trade union membership

(e) genetic data

(f) biometric data

(g) data concerning health

(h) data concerning a natural person's sex life or sexual orientation

3.2.2 where we are processing personal data relating to criminal convictions and offences on a large scale;

3.2.3 if we are carrying out systematic monitoring of a publicly accessible area such as through use of CCTV; or

3.2.4 where the Information Commissioner's Office requires a DPIA to be carried out. See www.ico.org.uk for details.

3.3 Even when a DPIA is not legally required, where we undertake a new project involving personal data our policy is that a consideration of privacy issues should be undertaken by carrying out a Short Form Privacy Review or a DPIA checklist (see Section 4 below).

3.4 For all new projects you must complete the DPIA checklist (available from the Legal Department) to determine whether a DPIA or a Short Form Privacy Review is required.

3.5 A copy of the completed DPIA checklist or Short Form Privacy Review must be retained a copy sent to the Legal Department and saved for audit purposes.

3.6 The DPIA checklist or Short Form Privacy Review must be completed prior to commencement of the project so that all privacy risks can be identified and mitigated before any data processing is carried out.

3.7 If a DPIA or Short Form Privacy Review is required, you must follow the steps set out in paragraph 4 below.

## 4 How do I undertake a DPIA/Short Form Privacy Review?

4.1 The following steps need to be taken to complete a DPIA/Short Form Privacy Review:

4.1.1 Complete the Short Form Privacy Review or the DPIA as applicable. Template documents for completion are available from the Legal Department.

4.1.2 Identify and document key privacy risks and the steps that will be taken to mitigate the identified risks in a Short Form Privacy Review or DPIA as applicable.

4.1.3 Obtain sign-off for the DPIA or Short Form Privacy Review from the relevant project sponsor/manager.

4.1.4 Identify who will take responsibility for ensuring that all mitigating steps identified through the DPIA or Short Form Privacy Review are implemented in practice.

4.1.5 Identify appropriate reporting periods to ensure that the identified mitigating steps have been implemented.

## 5 Who is responsible for completing the Data Protection Impact Assessment or Short Form Privacy Review?

5.1 The project sponsor is responsible for ensuring that the DPIA or Short Form Privacy Review is completed. For projects where a DPIA is required the project sponsor must obtain input from the Legal Department when completing the DPIA.

5.2 If a third party is involved in the project it may also be appropriate to seek the third party's input into the DPIA. For example, if a third party system is being procured, the vendor is likely to be best placed to provide information about the security elements of the system, its capabilities to delete or extract data etc.

## 6 Retention and storage

6.1 The Information Commissioner's Office may request a copy of a DPIA and therefore a copy of any DPIA undertaken must be retained by the Legal Department.