DATA PROTECTION POLICY

Governance and Business Improvement Manager

Contents

Policy	Data Protection Policy							
Version reference	V1							
Approved by	Board of Management							
Date of Approval	December 2024							
Review Period	3 years							
Review Due	December 2027							
Policy Review	Director of Finance & Business Support							
Who this policy affects	Board	X	Customers	X	Contractors	X	Members of the Public	X
Where this policy affects	General needs	X	Supported	X	Office / staff base	X		

1. Introduction

1.1 Almond Housing Association (referred to herein as AHA) is a Data Controller registered with the Information Commissioner's Office (Registration No: **Z4868537**). AHA's subsidiary, Almond Enterprises Ltd, is also a Data Controller registered with the Information Commissioner's Office (Registration No: **Z3475588**).

1.2 AHA is committed to ensuring the lawful, fair and transparent management of personal data. This policy sets out how we will do this.

1.3 All directors, officers associates, members, employees, volunteers (referred to herein as 'AHA personnel') have a responsibility to ensure compliance with this policy which sets out AHA's commitment to process personal data in accordance with the relevant legislation including:

- UK General Data Protection Regulation.
- UK Data Protection Act 2018 (DPA 2018).
- Privacy and Electronic Communications Regulations 2003 (PECR).

2. Scope

2.1 This Policy applies to all personal data held by AHA that relates to living identifiable individuals regardless of the category of data or the format of the data. Personal data is any data which could be used to identify a living individual including, for example, name, address, email, postcode, CCTV image and photograph and video recordings.

2.2 Special Category personal data is any information relating to racial or ethnic origin, political opinions, religious beliefs, health (mental and physical), sexual orientation, Trades Union membership and criminal convictions.

2.3 This policy applies to personal data held or accessed on AHA premises and systems or accessed remotely via home or mobile working. Personal data stored on personal and removable devices is also covered by this policy.

3 Responsibilities for compliance

3.1 The Board and Chief Executive are ultimately responsible for ensuring that AHA meets its legal obligations in respect of data protection legislation. The Board's responsibility is to ensure that AHA has an approved policy, Privacy Notices and to monitor implementation of the policy and deal with any matters arising from the policy that require Board decision. The Chief Executive has overall responsibility for ensuring that all employees comply with data protection legislation by implementing and supporting the policy.

3.2 Failure to comply with data protection legislation could lead to financial penalties, regulatory action, as well as reputational damage.

3.3 All AHA personnel, accessing or otherwise processing personal data controlled by AHA have a responsibility for ensuring personal data is collected, stored and handled appropriately and must ensure that it is handled and processed in compliance with data protection law, this policy and the data protection principles.

3.4 The Data Protection Officer, is responsible for:

- monitoring compliance with this policy and data protection legislation;
- managing personal data breaches and data subject rights requests;
- recording and maintaining appropriate records of processing activities and the documented evidence required for compliance.

4. Compliance

4.1 AHA will comply with its legal obligations and the data protection principles by ensuring that personal data is:

- processed lawfully, fairly and in a transparent manner in relation to individuals. Individuals will be advised on the reasons for processing via a Privacy Notice. Where data subjects' consent is required to process personal data, consent will be requested in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Data Subjects will be advised of their right to withdraw consent and the process for Data Subjects to withdraw consent will be simple.

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Personal data will only be used for the original purpose it was collected for and these purposes will be made clear to the data subject. If AHA wishes to use personal data for a different purpose, for example for research, the data subject will be notified prior to processing.

- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. AHA will only collect the minimum personal data required for the purpose. Any personal data deemed to be excessive or no longer required for the purposes collected for will be securely deleted in accordance with AHA's Retention Policy. Any personal information that is optional for individuals to provide will be clearly marked as optional on any data collection forms.

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay. AHA will take reasonable steps to keep personal data up to date, where relevant, to ensure accuracy. Any personal data found to be inaccurate will be updated promptly. Any inaccurate personal data that has been shared with third parties will also be updated.

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. AHA will hold data for the minimum time necessary to fulfil its purpose. Timescales for retention of personal data will be stated in a Retention Schedule. Data will be disposed of in a responsible manner ensuring confidentiality and security.

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. AHA will implement appropriate security measures to protect personal data. Personal data will only be accessible to those authorised to access personal data on a 'need to know' basis. AHA personnel will keep data secure by taking sensible precautions and following the relevant AHA policies and procedures relating to data protection.

4.2 In addition, AHA will comply with the 'Accountability Principle' that states that organisations are to be responsible for, and be able to demonstrate, compliance with the above principles.

5. Data sharing

5.1 In certain circumstances AHA may share personal data with third parties. This may be part of a regular exchange of data, one-off disclosures or in unexpected or emergency situations. In all cases, appropriate security measures will be used when sharing any personal data.

5.2 Where data is shared regularly, a contract or data sharing agreement will be put in place to establish what data will be shared and the agreed purpose.

5.3 Prior to sharing personal data, AHA will consider any legal implications of doing so.

5.4 Data Subjects will be advised of data sharing via the relevant Privacy Notice.

6. Data processor

6.1 Where AHA engages Data Processors to process personal data on its behalf, it will ensure that:

- Data processors have appropriate organisational and technical security measures in place.
- No sub-processors are used without prior written consent from AHA.
- An appropriate contract or agreement is in place detailing the obligations and requirements placed upon the data processor.

7. Security incident and breach management

7.1 Occasionally AHA may experience a data security incident or personal data breach; this could be if personal data is:

- Lost: for example, misplacing documents or equipment that contain personal data through human error; via fire, flood or other damage to premises where data is stored.
- Stolen: theft or as a result of a targeted attack on the IT network (cyber-attack).
- Accidently disclosed to an unauthorised individual: for example, email or letter sent to the wrong address.
- Inappropriately accessed or used.

7.2 All security incidents or personal data breaches will be reported to and managed by AHA's Data Protection Officer.

7.3 The Information Commissioner's Office and the individuals affected will be notified promptly, if required.

7.4 All security incidents and personal data breaches will be managed in accordance with AHA's Personal Breach Management Procedure (Appendix 1).

7.5 To assist with the prevention of personal data breaches, all AHA personnel must adhere to AHA's information security policies and procedures.

8. Individual Rights

8.1 AHA will uphold the rights of data subjects to access and retain control over their personal data in accordance with its Data Protection and Access to Personal Information Procedure. AHA will comply with individuals':

- **Right to be Informed** – by ensuring individuals are informed of the reasons for processing their data in a clear, transparent and easily accessible form and informing them of all their rights.
- **Right to Access** – by ensuring that individuals are aware of their right to obtain confirmation that their data is being processed; access to copies of their personal data and other information such as a privacy notice and how to execute this right.
- **Right to Rectification** – by correcting personal data that is found to be inaccurate. AHA will advise data subjects on how to inform us that their data is inaccurate. Inaccuracies with be rectified without undue delay.
- **Right to Erasure** (sometimes referred to as 'the right to be forgotten') – AHA will advise data subjects of their right to request the deletion or removal of personal data where processing is no longer required or justified.
- **Rights to Restrict Processing** – AHA will restrict processing when a valid request is received by a data subject and inform individuals of how to exercise this right.

- **Right to Data Portability** – by allowing, where possible, data to be transferred to similar organisation in a machine-readable format.

- **Right to Object** – by stopping processing personal data, unless legitimate grounds can be demonstrated for the processing which override the interest, rights and freedoms of an individual, or the processing is for the establishment, exercise or defence of legal claims.

9. Data protection by design

9.1 AHA has an obligation to implement technical and organisational measures to demonstrate that data protection has been considered and integrated into its processing activities.

9.2 When introducing any new type of processing, particularly using new technologies, it will take account of whether the processing is likely to result in a high risk to the rights and freedoms of individuals and consider the need for a Data Protection Impact Assessment (DPIA).

9.3 All new policies including the processing of personal data will be reviewed by the Data Protection Officer to ensure compliance with the law and establish if a DPIA is required. Advice and assistance will be provided by the DPO and if it is confirmed that a DPIA is required, it will be carried out in accordance with AHA's DPIA Procedure – appended to this policy.

10. Training

10.1 All AHA personnel will be made aware of good practice in data protection and where to find guidance and support for data protection issues. Adequate and role specific data protection training will be provided during induction and annually thereafter to everyone who has access to personal data to ensure they understand their responsibilities.

11. Breach of policy

11.1 Any breaches of this policy may be dealt with in accordance with AHA's disciplinary procedures.

12. Monitoring and reporting

12.1 Monitoring and audits may be undertaken by the Data Protection Officer to check compliance with the law, this policy and associated procedures. Any concerns will be raised with Senior Management/Board.

13. Equality, Diversity & Inclusion

13.1 Almond aims to ensure that equality, fairness, dignity and respect are central to the way we work and how we treat our customers. We support diversity and uphold equal opportunities in all areas of our work as an employer and service provider.

13.2 Almond will not discriminate against tenants, staff, visitors, suppliers or others based on their age, sex, sexual orientation, race, disability, religion or belief, marital status, pregnancy and maternity or gender reassignment (collectively referred to as 'protected characteristics' in the Equality Act 2010).

14. Data Protection

14.1 Our policies and procedures foster an approach of 'data protection by design and by default'. What this means in practice is that:

- Policies and procedures consider data protection issues, ie how to protect the data subject served by the policy or procedure;
- New systems, services, products and business practices involving personal data are designed and implemented to ensure personal data is protected by default;
- That the Data protection principles and safeguarding of individuals' rights (such as data minimisation, pseudo anonymisation, and purpose limitation) are clear in the policy or procedure;
- And that if the policy or procedure aims to provide service to vulnerable groups (e.g. children) that the personal data is treated with extra protection.

What this requires users of this policy to do is:

- Make sure that staff understand why data protection is important for the implementation of this policy, for instance via training or by reading the data protection policies;
- If we are undertaking a review of the policy, change to process or change to system, that we must consider doing a Data Protection Impact assessment, if the change is likely to result in a high risk to individuals.
- It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

We will consult our data protection officer, if there is doubt over these requirements.

15. Policy Review

15.1 This policy will be reviewed every three years or as required due to legislative or regulatory change. The review will be completed by December 2027 and circulated to the Board of Management for approval.

16. Associated Policies & Guidance

16.1 This Policy takes account of the following documents:

- UK General Data Protection Regulations
- Data Retention Policy and Schedule
- CCTV Policy
- Use of CCTV System Procedure
- Personal Data Breach Management Procedure
- Data Protection Impact Assessment procedure
- IT security policies and procedures
- Records Management Policy
- Data Protection and Access to Personal Information Procedure
- Document Management (Off site Storage) Procedure

17. Responsibilities Chart

17.1 The chart below illustrates the responsibilities of all staff in relation to this policy.

	Board	CEO	Director of Finance & Business Support	Governance Manager	All Staff
To Implement the policy		✓		✓	
Ensure Almond HA staff have an understanding of Policy				✓	
Policy Review			✓	✓	
Ensure Policy Reviewed	✓				
Ensure Equality & Diversity guidance is adhered to					✓
Appeals process	✓				

Policy Assessment Checklist

Health & Safety Assessment

Does this policy have the potential to affect:

	Yes	No
Lone Working	☐	☒
Safety and/or wellbeing of customers	☐	☒
Safety and/or wellbeing of staff	☐	☒

Equality Impact Assessment

Does this policy have the potential to affect:

	Yes	No
Age	☐	☒
Disability	☐	☒
Gender reassignment	☐	☒
Marriage and Civil Partnership	☐	☒
Pregnancy and Maternity	☐	☒
Religion or belief	☐	☒
Sex	☐	☒
Sexual orientation	☐	☒
Race	☐	☒

If you have answered 'Yes' to any of these points, please complete a full Equality Impact Assessment. If you have answered 'No', you need take no further action in completing an Equality Impact Assessment.

Data Protection Impact Assessment

Carrying out a Data Protection Impact Assessment [DPIA] will be useful to any project – large or small – that:

- Involves personal or sensitive data about individuals
- May affect our customers' reasonable expectations relating to privacy
- Involves information that may be used to identify or target individuals

A Data Protection Impact Assessment [DPIA] must be completed if the policy involves one or more of the following (please tick each that apply to this policy):

Evaluation or scoring	☐
Automated decision-making with significant effects;	☐
Systematic monitoring	☐
Processing of sensitive data or data of a highly personal nature	☐
Processing on a large scale	☐
Processing of data concerning vulnerable data subjects	☐
Innovative technological or organisational solutions	☐
Processing that involves preventing data subjects from exercising a right or using a service or contract	☐
Use systematic and extensive profiling or automated decision-making to make significant decisions about people	☐
Process special-category data or criminal-offence data on a large scale	☐
Systematically monitor a publicly accessible place on a large scale	☐
Use of new technologies involving significant innovation	☐
Use profiling, automated decision-making or special category data to help Make decisions on someone's access to a service, opportunity or benefit	☐
Carry out profiling on a large scale	☐
Process biometric or genetic data	☐
Combine, compare or match data from multiple sources	☐
Process personal data without providing a privacy notice directly to the individual	☐
Process personal data in a way that involves tracking individuals' online or offline location or behaviour	☐
Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them	☐
Process personal data that could result in a risk of physical harm in the event of a security breach	☐
There is a change to the nature, scope, context or purposes of our processing	☐

If a DPIA is not carried out, please summarise the reasons below

This policy describes how personal data is to be processed and managed in accordance with data protection legislation and ensures we remain compliant.

Appendix 1- Personal Data Breach Management

What is a Personal Data Breach?

A personal data breach is a security incident (as outlined above) leading to the **destruction, loss, alteration, unauthorised disclosure of, or access to, personal data**. It is important to understand that a personal data breach is more than just losing personal data.

Essentially while all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches.

Roles and Responsibilities All at AHA

Personnel

- Reporting any security incidents to the Data Protection Officer
- Assisting with any investigation
- Implementing any actions to contain and recover information

Data Protection Officer

- Recording all security incidents
- Deciding if incident has resulted in a personal data breach
- Manage investigations and actions to contain and recover information
- Notify the relevant staff, ICO, data subjects
- Identify lessons learned and implement actions to reduce future re-occurrence.

Board/Senior Management Team

- Ensure appropriate resources are allocated to assist in breach investigations, containment and recovery
- Review Breach Register and reports

Reporting a Security Incident

It is the responsibility of all personnel to report any suspected or actual Security Incident as soon as possible to the Data Protection Officer at the latest the next working day. It is vital that the Data Protection Officer is notified of the incident promptly in order to ensure AHA takes all immediate actions available to reduce the impact of the incident, identify if personal data is involved and if notification is required to the Information Commissioners Office (ICO) or any relevant data subjects.

You should report any incident by contacting the Data Protection Officer, and follow up with an email to the DPO if you are unable to make direct contact.

Where an incident involves data or ICT systems the Data Protection Officer will notify the ICT Manager as soon as possible.

If an incident is identified out of office hours (over weekends/office closures) this should be reported at the earliest opportunity to the Director of Finance and Business Support.

AHA may also be required to report any security incidents to our regulatory authority(ies).

Containment & Recovery

An Incident requires investigation promptly to contain the situation and also a recovery plan including, where necessary, damage limitation. This will often involve input from across the organisation.

The following will be established:

- Who is required to investigate the breach with the DPO and what resources will be required. In cases involving ICT systems, this will often be the ICT Manager.

- Who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. *(This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.)*

- Whether there is anything we can do to recover any losses and limit the damage the breach could cause. (*As well as the physical recovery of equipment, this could involve the use of back-ups to restore lost or damaged data or ensuring that personnel recognise when someone tries to use stolen data to access accounts.)*

- If criminal activity is suspected the Police may be informed depending on the incident.

Assessing the Risks

Some data security incidents will not lead to risks beyond possible inconvenience to those who need the data to do their job. For example, where a laptop is irreparably damaged, but its files were backed up and can be recovered, albeit at some cost to the business.

While these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of a customer database, the data on which may be used to commit identity fraud.

Before deciding on what steps are necessary further to immediate containment, assess the risks which may be associated with the incident. Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

The following will be used to make an assessment:

- What type of data is involved? *If it includes personal data it will be considered a Personal Data Breach.*
- How sensitive is it? *Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)*
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate or the organisation; if it has been damaged, this poses a different type and level of risk
- Regardless of what has happened to the data, what could the data tell a third party about an individual or the organisation? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts

of data but is certainly an important determining factor in the overall risk assessment
- Who are the individuals whose data has been breached? Whether they are staff or tenants, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks
- What harm can come to individuals or the organisation? Are there risks to physical safety or reputation, of financial loss or a combination of these?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service we provide?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

Notification

Notification to ICO

AHA has to notify the ICO of a personal data breach (via the DPO) where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed, such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Incidents have to be assessed on a case by case basis. For example, we will need to notify the ICO about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

Appendix A provides examples of what breaches require notification and to whom.

The decision to notify the ICO will be made by Data Protection Officer. A written record of this decision will be recorded in the Breach Register.

Information to be provided to the ICO

The nature of the personal data breach including, where possible: the categories and approximate number of individuals concerned; and the categories and approximate number of personal data records concerned.

The name and contact details of the Data Protection Officer or other contact point where more information can be obtained.

A description of the likely consequences of the personal data breach. A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

How to notify the ICO

A notifiable breach has to be reported to the ICO within 72 hours of us becoming 'aware' of it. When we become 'aware' of the breach is the point when we know or suspect there has been a personal data breach. We may not discover that a security incident is a personal data breach initially, but as soon as we do know or suspect that personal data is involved then we are 'aware'.

Some examples to help determine when we become aware:

- In the case of a loss of a CD/USB with unencrypted data it is often not possible to ascertain whether unauthorised persons gained access. Nevertheless, such a case has to be notified as there is a reasonable degree of certainty that a breach has occurred; we would become 'aware' when we realised the CD/USB had been lost.
- A third party informs us that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. As we have been presented with clear evidence of a breach then there can be no doubt that we have become 'aware'.
- We detect that there has been a possible intrusion into our network. We check our systems to establish whether personal data held on that system has been compromised and confirms this is the case. Once again, we now have clear evidence of a breach there can be no doubt that we have become 'aware'.

It is recognised that it will often be impossible to investigate a breach fully within the 72 hour time-period and legislation allows for us to provide information to the ICO in phases.

Delayed Notifications

If it is not possible to notify the ICO within 72 hours, when notification is completed it must include the reasons for the delay. We should always aim to notify the ICO as soon as possible even if we do not have much detail at that point.

Notification to Data Subjects

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

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we must notify those concerned directly and without undue delay, unless this would involve disproportionate effort.

If it is not possible to contact the data subjects directly or there is a large volume of data subjects involved, then we should make a public communication or similar measure whereby the data subjects are informed in an equally effective manner. Dedicated messages must be used when communicating a breach to data subjects and they should not be sent with other information, such as regular updates or newsletters. This helps to make the communication of the breach to be clear and transparent.

Examples of transparent communication methods include direct messaging (e.g. email, SMS), prominent website banners, social media posts or notification, postal communications and prominent advertisements in printed media.

Communicating a breach to data subjects allows us to provide information on the risks presented as a result of the breach and the steps the data subjects can take to protect themselves from its potential consequences.

Information to be provided to Data Subjects where notification is warranted

We must provide the following information:

- a description of the nature of the breach;
- the name and contact details of the Data Protection Officer or other contact point;
- a description of the likely consequences of the breach; and

- a description of the measures taken or proposed to be taken by us to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.
- If the data subject wishes to raise a complaint about the breach, this should be escalated to the Data Protection Officer.

Evaluation

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of our response to it once completed.

If it was identified that the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable. Also, if the management of the breach was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and lines of responsibility in the light of experience.

We may find that existing procedures could lead to another breach and you will need to identify where improvements can be made.

The Data Protection Officer will work with the relevant staff involved in the breach to review process and procedures, to ensure that effective measures have been taken to prevent a recurrence of the breach and to monitor ongoing compliance.

The Data Protection Officer will publicise any identified learning outcomes to all parties who may benefit from the updated guidance or information.

Records Management

A Breach Register will be maintained by the Data Protection Officer and this will be reported to the Board on an annual basis.

A case file will be made for each investigation to ensure a full record of the investigation, any correspondence, and decisions on notifications, are maintained accurately and retained as per the AHA Data Retention Schedule.

Monitoring and Reporting

Regular monitoring and audits may be undertaken by the DPO to check compliance with the law, this policy and associated procedures. Any concerns will be raised with the Board/Senior Management Team.

Policy Review

This procedure will be reviewed every three years or when required to address any weakness in the procedure or changes in legislation or best practice.

Appendix A – Notification Guidance

Examples of personal data breaches and who to notify.

The following non-exhaustive examples will assist in determining whether we need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	Notify the ICO	Notify the Data Subject(s)	Notes
A controller stored a backup of an archive of personal data encrypted on a CD. The CD is stolen during a break-in	No	No	As long as the data are encrypted with a state of the art algorithm, backups of the data exist, and the unique key is not compromised, this may not be a reportable breach. However, if it is later compromised, notification is required
Personal data of individuals are infiltrated from a secure website managed by the controller during a cyber-attack.	Yes, report to ICO if there are potential consequences to individuals	Yes, depending on the nature of the personal data affected and if the severity of the potential consequences to individuals is high	If the risk is not high, we recommend the controller to notify the data subject, depending on the circumstances of the case. For example, notification may not be required if there is a confidentiality breach for a newsletter related to a TV show, but notification may be required if this newsletter can lead to political point of view of the data subject being disclosed
A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No	No	This is not a notifiable personal data breach, but still a recordable incident. Appropriate records should be maintained by the controller
A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system	Yes, report to the ICO, if there are potential consequences to individuals as this is a loss of availability	Yes, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences	If there was a backup available and data could be restored in good time, this would not need to be reported to the ICO or to individuals as there would have been no permanent loss of availability or confidentiality. However, the ICO may consider an investigation to assess compliance with the broader security requirements

An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and if it is a systemic flaw so that other individuals are or might be affected	Yes	Only the individuals affected are notified if there is high risk and it is clear that others were not affected	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them
Personal data of 5000 students are mistakenly sent to the wrong mailing list with 1000+ recipients	Yes	Yes, depending on the type of personal data involved and the severity of possible consequences	
A direct marketing e-mail is sent to recipients in "to:" or "cc:" field, thereby enabling each recipient to see the email address of other recipients	Yes, notifying the ICO may be obligatory if a large number of individuals are affected, if sensitive data are revealed	Yes, depending on the type of personal data involved and the severity of possible consequences	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

Personal Data Breach Reporting Form

To be completed by the person in the organisation who is aware of the circumstances of the breach. It is important to note as much information as you have regarding any breach or suspected breach. Contact DPO for assistance with completion of form.

What has happened? Tell us as much as you can about what happened, what went wrong and how it happened.

Was the breach caused by a cyber incident?

Yes/No

How did you find out about the breach?

When did you discover the breach?

Date:
Time:

When did the breach happen?

Date:
Time

If there has been a delay in reporting this breach, please explain why.

Categories of personal data included in the breach (tick all that apply)

☐ Data revealing racial or ethnic origin
☐ Political opinions
☐ Religious or philosophical beliefs
☐ Trade union membership
☐ Sex life data
☐ Sexual orientation data
☐ Gender reassignment data
☐ Health data
☐ Basic personal identifiers, eg name, contact details
☐ Identification data, eg, username, passwords
☐ Economic and financial data, eg credit card numbers, bank details
☐ Official documents, eg driving licenses, passports
☐ Location data eg GPS position
☐ Criminal convictions, offences
☐ Genetic or biometric (fingerprint or iris recognition) data
☐ Not yet known
☐ Other (please give details below)

Number of personal data records concerned?

How many data subjects could be affected?

Potential consequences of the breach. *Please describe the possible impact on data subjects, as a result of the breach. Please state if there has been any actual harm to the data subjects.*

Categories of data subjects affected (tick all that apply)

☐ Employees
☐ Users of technology equipment
☐ Subscribers
☐ Customers or prospective customers
☐ Children
☐ Vulnerable adults
☐ Not yet known
☐ Other (please give details below)

Are the data subjects aware of the breach?

Yes/No
If you answered yes, please specify

Have the staff members involved in this breach received data protection training?

Yes/No

If yes – when?

Person making this incident notification report

Name:
Job Role:
Email:
Date:

When completed, please return this form to the Data Protection Officer

Cyber incidents only (completed by ICT Manager):

Has the confidentiality, integrity and/or availability of our information systems been affected?

Yes/No

If you answered yes, please specify (tick all that apply)

☐ Confidentiality
☐ Integrity
☐ Availability

What is the likely impact on our organisation?

CCTV POLICY

Governance and Business Improvement Manager

CCTV Policy

1. Introduction

1.1 AHA owns and operates CCTV and other forms of surveillance systems at various premises, including server room in offices. We do this for the purpose of enhancing security where we consider there to be a potential threat to the health, safety and wellbeing of individuals and to assist in the prevention and detection of risk of crime or anti-social behaviour.

1.2 AHA acknowledges the obligations it incurs in operating such systems and the rights and freedoms of those whose images may be captured. We are committed to operating them fairly and within the law at all times and in particular will comply with the requirements of the UK General Data Protection Regulations (the 'UK GDPR') and UK Data Protection Act 2018 (the 'DPA 2018'). In developing this document, AHA has incorporated the standards and practices from the Information Commissioner's Office Code of Practice, 'In the picture: A data protection code of practice for surveillance cameras and personal information' as well as the Surveillance Camera Commissioner Code of Practice 'A guide to the 12 principles'

1.3 This policy governs AHA approach to installing and operating CCTV and other forms of surveillance systems and handling the information obtained. It is underpinned by the following key principles:

- Know we what the system is used for and review of its use;
- That we have completed a Data Protection Impact Assessment (DPIA) for the use of CCTV. Systems will only be installed with due consideration to the privacy impacts of doing so;
- That we will ensure clear signage is in place, with a published point of contact to deal with queries and complaints;
- There is clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used, and staff are aware of their responsibilities for CCTV;
- Clear rules, policies and procedures are in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them;
- That we have a policy for keeping the CCTV images we hold, and we ensure they are deleted once they are no longer needed;
- That we have a clear process for who can access the images,
- That the system we use follows recognised operational and technical standards. Systems will be appropriately specified and professionally installed, having due regard to appropriate technical and legal advice and other relevant guidance;
- Systems will only be installed where there is a clear identified and documented need;

- Systems will only be installed with due consideration to all alternative options;
- Appropriate technical and organisational measures will be employed to ensure the security of our systems and personal data, including relevant controls to govern access to and use of images;
- Appropriate measures will be taken to provide clear and accessible privacy information to individuals whose personal data is processed by systems;
- That we are clear on when CCTV images will be produced for criminal justice purposes;
- This policy will be supplemented by procedures, which provide detailed operational guidance on the installation, operation, use and maintenance of our systems.

2. Decisions on Installing CCTV and Surveillance Systems

2.1 AHA recognises that using CCTV and other surveillance systems can be privacy intrusive. As such it will not install systems as a routine response to incidents of a criminal or anti-social nature. Notwithstanding this, we acknowledge the potential value of these systems as both a deterrent and a means of detection and will consider all potential installations on a case- by-case basis. In doing so the aim will be to demonstrate that installation is a justified, proportionate and effective solution to an identified problem or risk.

2.2 The impact on people's right to privacy and the availability of alternative and less intrusive options will be a key consideration. To this end, all potential installations will be subject to a Data Protection Impact Assessment (DPIA). All DPIAs will be conducted, recorded and signed off in accordance with our DPIA procedures. These have been developed in accordance with Information Commissioner's Office (ICO) guidance and prescribe the approach to be followed in identifying and assessing data protection risks, and in consulting with those whose privacy is likely to be affected, where appropriate. AHA Data Protection Officer will advise on and review DPIAs as required.

3. System Specification and Installation

3.1 AHA will procure site systems in accordance with an agreed standard specification, which reflects recommended practices and incorporates privacy by design features. Relevant criteria will include, but not be limited to:

- Ensuring personal data can be easily located and extracted;
- Ensuring images are of an appropriate quality, relevant to their purpose;
- Ensuring that the date and time images are captured is easily identifiable;
- Ensuring that unnecessary images are not viewed or recorded;
- Ensuring that relevant retention periods can be complied with;

- Installing image only systems, which have no sound recording capability, as standard;
- Siting cameras to ensure only areas of interest are subject to surveillance and to minimise viewing areas not relevant to the purposes the system was installed for, with due regard given to planning permission requirements as necessary;
- Siting cameras to ensure they can produce quality images taking into account the environment where located;
- Siting cameras and equipment in secure locations, protected from unauthorised access and possible vandalism; and
- No cameras forming part of the system will be installed in a covert manner; and cameras which may be covered to protect them from weather or damage, would not be regarded as covert provided that appropriate signs are in place.

3.2 AHA will engage the services of specialist contractors, in accordance with relevant procurement procedures, to advise on technical specifications and system configuration and design; and to carry out installation and maintenance. Such contractors will be required to demonstrate the appropriate credentials, expertise, and understanding of AHA and data protection requirements.

3.3 AHA will maintain a register of all system installations, detailing location and installation date, relevant technical specifications and system design features.

4. Access and Use of Images

4.1 Access to all equipment and images will be strictly controlled. Appropriate security measures will be in place to ensure entry to physical locations is limited to authorised personnel. As a general rule, such authorised personnel will be individuals appointed by AHA, specialist contractors, acting under explicit instruction. AHA will have in place a written data processing agreement with these contractors which is UK GDPR compliant and clearly defines obligations, responsibilities and liabilities.

4.2 The specialist contractors will be responsible for setting and maintaining relevant technical security controls for each system, including passwords or access codes and for maintaining physical and digital access logs.

4.3 AHA considers the following to be permitted reasons for monitoring:

- Prevention and detection of unacceptable behaviour, including aggressive or abusive actions, towards staff in AHA premises;
- Prevention and detection of unauthorised access to, or other criminal activity within, AHA premises; and/or
- General compliance with relevant legal obligations, regulatory requirements and AHA policies and procedures.

4.4 AHA shall not undertake routine monitoring of images captured in AHA locations.

4.5 Access to images will be on an as required basis and in accordance with the purpose for which the system was installed. This will only be carried out where an incident has been reported that requires investigation or where there is clear suspicion that an incident has taken place. Where it is required to access or download recorded images in order to investigate an alleged incident a data request, authorised as a minimum by the relevant Manager, this will be recorded in the CCTV manual log book.

4.6 Access to images may also be required in order to respond to a Subject Access Request (SAR). All requests for system footage by individuals will be treated as SARs and handled in line with AHA SAR Procedures. In doing so AHA acknowledges the requirement to balance the rights of data subjects against those of other individuals who appear in the requested images. On receipt of a SAR, arrangements will be made to retain, and prevent automatic deletion of, all images of the individual submitting the SAR that have been captured.

4.7 Access to CCTV images will be dealt with in line with AHA's Data Protection and Access to Personal Information procedure and Use of CCTV System procedure.

4.8 Disclosure of information from systems will be controlled and consistent with the purpose(s) for which the system was installed. As such disclosure is likely to be limited to law enforcement agencies or the AHA legal advisers. The CCTV log will contain relevant details of image disclosure, including named recipient and reason for disclosure. Any disclosure of images must be done by secure means.

4.9 AHA will not routinely keep copies of images obtained through CCTV or other surveillance systems. Any images that are returned following disclosure will be disposed of securely in accordance with AHA Data Retention and Destruction Policy and Procedures.

4.10 AHA considers any attempted or actual misuse of CCTV or other surveillance systems or images by staff members to be a disciplinary matter, which will be handled in accordance with the relevant policy and procedures.

4.11 AHA will consider requests from Police and other legal authorities when suitable reasons have been given and that are in line with their obligations under the Investigatory Powers Act 2016. Such disclosure of information must follow our disclosure procedure.

5. Reviewing Installations

5.1 As a minimum, each system will be reviewed 6 months after initial installation and every 12 months thereafter to ensure its continued use serves a legitimate purpose and is required; and that the installation specification and design is appropriate to this purpose. This will involve a

review and, as necessary, an update of the DPIA to reflect changes or actions required.

5.2 Where it is determined that a system is no longer needed, arrangements for decommissioning will be made promptly. This will involve removal of all cameras and associated equipment and signage in accordance with AHA CCTV and surveillance system procedures.

5.3 Notwithstanding these regular reviews, AHA will separately instruct its contractors to undertake periodic maintenance and security checks. Any works to repair or replace system components, or to amend system configuration or design will be carried out only under explicit instruction.

6. Privacy Information

6.1 AHA shall be as transparent as possible in its usage of CCTV and surveillance systems and AHA Privacy Notices will reference the collection of personal data via systems. Clear and prominent signage will also be in place where systems are in operation. Signage requirements will be included as part of the standard system specification, and the appointed specialist contractors will be required to confirm these have been met as part of the installation process.

6.2 AHA acknowledges that individuals also have the right to complain to the Information Commissioner's Office (ICO) directly if they feel AHA is not operating CCTV and surveillance systems in accordance with the UK GDPR and/or DPA 2018.

7. Review

This policy will be reviewed every three years as part of a review of the Data Protection Policy, or sooner if required by changes in legislation or regulatory guidance.

DATA PROTECTION IMPACT ASSESSMENT (DPIA) PROCEDURE

Governance and Business Improvement Manager

Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment ('DPIA') is a tool to help us identify and minimise the data protection risks of new projects. They are part of our accountability obligations under the UK General Data Protection Regulation, and an integral part of the 'data protection by default and by design' approach.

We must do a DPIA for certain types of processing of personal data, or any other processing that is likely to result in a high risk to individuals.

A DPIA must:

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

To assess the level of risk, we must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

The Data Protection Officer will be consulted when completing a DPIA and where appropriate, individuals and relevant experts. Any data processors may also need to assist in completing it.

If we identify a high risk that we cannot mitigate, we must consult the Information Commissioner's Office ('ICO') before starting the processing.

An effective DPIA helps us to identify and fix problems at an early stage, demonstrate compliance with our data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur.

This procedure explains the principles and process that form the basis of a DPIA. It helps us to understand what a DPIA is for, when we need to carry one out, and how to go about it.

What is a DPIA?

A DPIA is a process designed to help us systematically analyse, identify and minimise the data protection risks of a project or planned change. It is a key part of our accountability obligations under the UK GDPR, and when done properly helps us assess and demonstrate how we comply with all of our data protection obligations.

It does not have to eradicate all risk, but should help us minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what we want to achieve.

DPIAs are designed to be a flexible and scalable tool that we can apply to a wide range of projects regardless of size. Conducting a DPIA does not have to be complex or time-consuming in every case, but there must be a level of strictness in proportion to the privacy risks arising.

Why are DPIAs Important?

DPIAs are an essential part of our accountability obligations. Conducting a DPIA is a legal requirement for any type of processing that is likely to result in high risk (including certain specified types of processing). Failing to carry out a DPIA in these cases may leave us open to enforcement action, including a fine of up to £10 million or 2% annual turnover.

A DPIA also brings broader compliance benefits, as it can be an effective way to assess and demonstrate our compliance with all data protection principles and obligations. However, DPIAs are not just a compliance

exercise. An effective DPIA allows us to identify and fix problems at an early stage, bringing broader benefits for both individuals and Almond HA.

It can reassure individuals that we are protecting their interests and have reduced any negative impact on them as much as we can. In some cases the consultation process for a DPIA gives them a chance to have some say in the way their information is used.

Conducting and publishing a DPIA can also improve transparency and make it easier for individuals to understand how and why you are using their information.

In turn, this can create potential benefits for our reputation and relationships with individuals:

- help us to build trust and engagement with the people using our services, and improve our understanding of their needs, concerns and expectations;
- identifying a problem early on generally means a simpler and less costly solution, as well as avoiding potential reputational damage later on; and
- reduce the ongoing costs of a project by minimising the amount of information we collect where possible and devising more straightforward processes for staff.

In general, consistent use of DPIAs increases the awareness of privacy and data protection issues within Almond HA and ensures that all relevant staff involved in designing projects think about privacy at the early stages and adopt a '**data protection by design'** approach.

How are DPIAs Used?

A DPIA can cover a single processing operation, or a group of similar processing operations. For new technologies, we may be able to use a DPIA done by the product developer to inform our own DPIA on our implementation plans.

For new projects, DPIAs are a vital part of data protection by design. They build in data protection compliance at an early stage, when there is most scope for influencing how the proposal is developed and implemented.

However, it's important to remember that DPIAs are also relevant if we are planning to make changes to an existing system. In this case we must ensure that we do the DPIA at a point when there is a realistic opportunity to influence those plans. A DPIA is not simply a rubber stamp or a technicality as part of a sign-off process. It's vital to integrate the outcomes of a DPIA back into any project plan. We should not view a DPIA as a one-off exercise to file away. A DPIA is a 'living' process to help us manage and review the risks of the processing and the measures put in place on an ongoing basis. We need to keep it under review and reassess if anything changes. In particular, if we make any significant changes to how or why you process personal data, or to the amount of data we collect, we need to show that our DPIA assesses any new risks.

An external change to the wider context of the processing should also prompt us to review our DPIA. For example, if a new security flaw is identified, new technology is made available, or a new public concern is raised over the type of processing we do or the vulnerability of a particular group of data subjects.

What Kind of 'Risk' do DPIAs Assess?

There is no explicit definition of 'risk' in the UK GDPR, but the various provisions on DPIAs make clear that this is about the risks to individuals' interests. This includes risks to privacy and data protection rights, but also effects on other fundamental rights and interests.

The focus is therefore on any potential harm to individuals. However, the risk-based approach is not just about actual damage and should also look at the possibility for more intangible harm. It includes any "significant economic or social disadvantage". The impact on society as a whole may also be a relevant risk factor. For example, it may be a significant risk if our intended processing leads to a loss of public trust. A DPIA must assess

the level of risk, and in particular whether it is 'high risk'. The UK GDPR is clear that assessing the level of risk involves looking at both the likelihood and the severity of the potential harm.

When do we Need to do a DPIA?

We must do a DPIA before we begin any type of processing which is "likely to result in a high risk". This means that although we have not yet assessed the actual level of risk we need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, the UK GDPR says you **must** do a DPIA if you plan:

Systematic and extensive profiling with significant effects: "any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person". **Large scale use of sensitive data:** **"**processing on a large scale of special categories of data referred to in Article 9(1) (See Appendix 2) or of personal data relating to criminal convictions and offences referred to in Article 10" **Public monitoring:** **"**a systematic monitoring of a publicly accessible area on a large scale".

The ICO has also published a list of the kind of processing operations that are likely to be high risk and also **require** a DPIA.

New technologies: processing involving the use of new technologies, or the novel application of existing technologies (including AI). **Denial of service:** Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data
Large-scale profiling: any profiling of individuals on a large scale.
Biometrics: any processing of biometric data.
Genetic data: any processing of genetic data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject.
Data matching: combining, comparing or matching personal data obtained from multiple sources.
Invisible processing: processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort.
Tracking: processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.
Targeting of children or other vulnerable individuals: The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.
Risk of physical harm: Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.

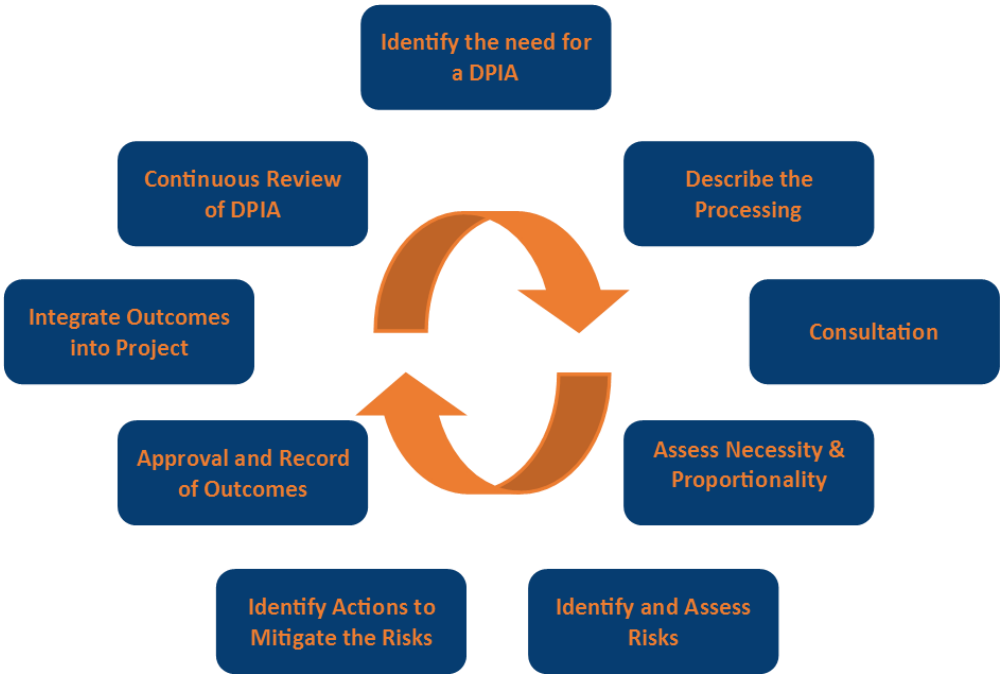
We should also think carefully about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals. Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving any use of personal data.

When deciding whether to do a DPIA, we should first answer the screening questions at Appendix 1.

After answering the screening questions, if the decision is made that a DPIA is needed, use the following guidance, as you go along, to complete the DPIA template at Appendix 3.

How to complete a DPIA

A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It should include these steps:



Responsibility for completing a DPIA

The project manager / lead would usually be best placed to conduct the required DPIA along with any other stakeholders who are able to input into the process.

The DPO will have a significant role in supporting the process, providing advice and guidance, will approve any completed assessment and where required liaise with the Information Commissioners Office.

Step 1: Identify the need for a DPIA

1.1 Contact the DPO and advise them of the new project/change.

1.2 Complete the DPIA Initial Screening Form (Appendix 1) to determine if you need to complete a DPIA.

1.3 If you decide that you do not need to do a DPIA, you should document the decision and the reasons for it on the DPIA Initial Screening Form (Appendix 1).

1.4 If you need to complete a DPIA you should use the DPIA Template (Appendix 3) and complete Step 1, where you should list the types of processing identified from the screening form, the aims of the project and why the need to complete a DPIA was identified.

Jump to Step 1 of the template

Step 2: Describe the Processing

2a Describe how and why you plan to use the personal data

The description must include "the nature, scope, context and purposes of the processing". The nature of the processing is what you plan to do with the personal data.

This should include, for example:

- how you collect the data;
- how you store the data;
- how you use the data;
- who has access to the data;
- who you share the data with;
- whether there are any data processors;
- retention periods;
- security measures;
- whether you are using any new technologies;
- whether you are using any novel types of processing; and
- which screening criteria you flagged as likely high risk.

2b The scope of the processing is what the processing covers.

This should include, for example:

- the nature of the personal data;
- the volume and variety of the personal data;
- the sensitivity of the personal data;
- the extent and frequency of the processing;
- the duration of the processing;
- the number of data subjects involved; and
- the geographical area covered.

2c The context of the processing **is the wider picture, including internal and external factors which might affect expectations or impact.**

This might include, for example:

- the source of the data;
- the nature of the relationship with the individuals (tenants, staff);
- the extent to which individuals have control over their data;
- the extent to which individuals are likely to expect the processing;

- whether they include children or other vulnerable people;
- any previous experience of this type of processing;
- any relevant advances in technology or security;
- any current issues of public concern.

2d The purpose of the processing **is the reason why you want to process the personal data.**

This should include:

- your legitimate interests, where relevant;
- the intended outcome for individuals; and
- the expected benefits for you or for society as a whole

Jump to Step 2 of the template

Step 3: Consultation

You should always seek the views of individuals (or their representatives) unless there is a good reason not to.

In most cases it should be possible to consult individuals in some form. However, if you decide that it is not appropriate to consult individuals then you should record this decision as part of the DPIA, with a clear explanation. For example, you might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.

If the DPIA covers the processing of personal data of existing contacts (for example, existing customers or employees), you should design a consultation process to seek the views of those particular individuals, or their representatives.

If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public consultation process, or targeted research. This could take the form of carrying out market research with a certain demographic or contacting relevant campaign or consumer groups for their views.

If your DPIA decision is at odds with the views of individuals, you need to document your reasons for disregarding their views.

Do you need to consult anyone else?

If the project involves a **data processor**, you may need to ask them for information and assistance.

You should consult all relevant internal stakeholders, the **IT Support Provider** if this is a new system or change to an existing system to allow Information Security to be considered.

In some circumstances we might also need to consult the ICO once you have completed your DPIA. (Explained in Step 6)

Jump to Step 3 of the template

Step 4: Assess Necessity and Proportionality

You should consider:

- Do your plans help to achieve your purpose?
- Is there any other reasonable way to achieve the same result?

The Article 29 guidelines also say you should include how you ensure data protection compliance, which are a good measure of necessity and proportionality.

In particular, you should include relevant details of:

- your lawful basis for the processing; (see Appendix 2 - Conditions of Processing)
- how you will prevent function creep;
- how you intend to ensure data quality;
- how you intend to ensure data minimisation;
- how you intend to provide privacy information to individuals;
- how you implement and support individuals' rights;
- measures to ensure your processors comply; and
- safeguards for any international transfers.

Jump to Step 4 of the template

Step 5: Identify and Assess Risks

Consider the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material.

In particular look at whether the processing could possibly contribute to:

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage

You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data). You may wish to discuss these with the IT Provider for electronic data transfers.

To assess whether the risk is a high risk, you need consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.

The below Risk Matrix must be considered when assessing likelihood and severity of harm to the rights and freedoms of the individual.

Severity of harm				
	Serious harm	Low risk	High risk	High risk
	Some harm	Low risk	Medium risk	High risk
	Minimal harm	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Jump to Step 5 of the template

Step 6: Identify Actions to Mitigate the Risks

Against each risk identified, record the source of that risk.

You should then consider options for reducing that risk.

For example:

- deciding not to collect certain types of data;
- reducing the scope of the processing;
- reducing retention periods;
- taking additional technological security measures;
- training staff to ensure risks are anticipated and managed;
- anonymising or pseudonymising data where possible;
- writing internal guidance or processes to avoid risks;
- adding a human element to review automated decisions;
- using a different technology;
- putting clear data sharing agreements into place;
- making changes to privacy notices;
- offering individuals the chance to opt out where appropriate; or
- implementing new systems to help individuals to exercise their rights.

This is not an exhaustive list, and you may be able to devise other ways to help reduce or avoid the risks.

Record whether the measure would reduce or eliminate the risk.

You should then record:

- what additional measures you plan to take;
- whether each risk has been eliminated, reduced, or accepted;
- the overall level of 'residual risk' after taking additional measures; and
- whether you need to consult the ICO.

You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation.

However, if there is still a high risk, you need to consult the ICO before you can go ahead with the processing.

When to Consult the ICO

If you have identified a high risk, and you cannot take any measures to reduce this risk, you need to consult the ICO. You cannot go ahead with the processing until you have done so. The focus is on the 'residual risk' after any mitigating measures have been taken. If the DPIA identified a high risk, but you have taken measures to reduce this risk so that it is no longer a high risk, you do not need to consult the ICO.

How do we consult the ICO?

The DPO will consult with the ICO on Almond HA's behalf. This is done by completing the online form.

The submission must include:

- a description of the respective roles and responsibilities of any joint controllers or processors;
- the purposes and methods of the intended processing;
- the measures and safeguards taken to protect individuals;
- a copy of the DPIA;

We will be notified if the DPIA has been accepted for consultation within ten days of sending it. If the ICO agree that a DPIA was required, they will review the DPIA.

They will consider whether:

- the processing complies with data protection requirements;
- risks have been properly identified; and
- risks have been reduced to an acceptable level.

The ICO will provide a written response, advising that:

- the risks are acceptable and you can go ahead with the processing;
- you need to take further measures to reduce the risks;
- you have not identified all risks and you need to review your DPIA;
- your DPIA is not compliant and you need to repeat it; or
- the processing would not comply with the GDPR and you should not proceed.

In some cases, the ICO may take more formal action. This might include an official warning not to proceed, or imposing a limitation or ban on processing.

If we disagree with the ICO advice we can ask for a review of the decision.

Jump to Step 6 of the template

Step 7: Approval and Record of Outcomes

As part of the approval process, you should submit your assessment to the Named Role/DPO to advise on whether the processing is compliant and can go ahead. If you decide not to follow their advice, you need to record your reasons.

Jump to Step 7 of the template

Step 8: Integrate Outcomes into Project

You must integrate the outcomes of your DPIA back into your project plans. You should identify any action points and who is responsible for implementing them.

You should monitor the ongoing performance of the DPIA. You may need to cycle through the process again before your plans are finalised.

It is good practice to publish DPIA's to aid transparency and accountability. This could help foster trust in our processing activities, and improve individuals' ability to exercise their rights.

Step 9: Continuous Review of DPIA

You need to keep your DPIA under review, and you may need to repeat it if there is a substantial change to the nature, scope, context or purposes of your processing.

.

DPIA Appendix 1 - DPIA Initial Screening Form

1. Project Details

Project Title / Change Description:	
Project Manager/ Lead details:	
Date of Screening:	

2. Answer yes or no to all the different types of processing listed below

Does the processing you are planning:	**Answer**
Use systematic and extensive profiling or automated decision making to make significant decisions about people?	
Process special category data (see Appendix 2) or criminal offence data on a large scale?	
Systematically monitor a publicly accessible place on a large scale?	
Use new technologies?	
Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?	
Carry out profiling on a large scale?	
Process biometric or genetic data?	
Combine, compare or match data from multiple sources?	
Process personal data without providing a privacy notice directly to the individual?	
Process personal data in a way which involves tracking individuals' online or offline location or behaviour?	
Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them?	
Process personal data which could result in a risk of physical harm in the event of a security breach?	

3. If the answer is **yes** to any one of these types of processing, then you **must** complete a DPIA. If the answer was **no** to all these types, then you must review the following processing listed below that may require a DPIA

Does the processing involve:	**Answer**
Evaluation or scoring	
Automated decision-making with significant effects	
Systematic monitoring	
Processing of sensitive data or data of a highly personal nature	
Processing on a large scale	
Processing of data concerning vulnerable data subjects.	
Innovative technological or organisational solutions	
Processing involving preventing data subjects from exercising a right or using a service or contract.	

4. If the answer is **yes** to any of these processing types you must discuss the requirement to complete a DPIA with the DPO.

Is DPIA Required?	
Reason for Decision if not completing DPIA:	

If the decision is made that a DPIA is needed, use the above guidance to complete the DPIA template at Appendix 3.

DPIA Appendix 2 – Conditions for Processing

Below are the different legal bases available for processing personal data and special categories of data.

Legal Bases for Processing Personal Data:

- 6(1)(a) – Consent of the data subject *(only use consent if there is no other condition that can be used)*
- 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- 6(1)(c) – Processing is necessary for compliance with a legal obligation
- 6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person
- 6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- 6(1)(f) – Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Categories of Special Category Data:

- Racial or ethnic origin
- Political opinion
- Religious or philosophical beliefs
- Trade Union membership
- Physical or mental health condition
- Sexual life and sexual orientation
- Genetic data
- Biometric data used to identify an individual

Conditions for Processing Special Categories of Data:

- 9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by law
- 9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
- 9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- 9(2)(d) – Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-pro fit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the

personal data are not disclosed outside that body without the consent of the data subjects.

- 9(2)(e) – Processing relates to personal data manifestly made public by the data subject
- 9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- 9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards
- 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of law or a contract with a health professional
- 9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- 9(2)(j) – Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

DPIA Appendix 3 - DPIA Template

Data Protection Impact Assessment

For guidance on how to complete this form, it is important to read the above DPIA Procedures before and during completion of this assessment.

This assessment must be commenced at the beginning of any project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes must be integrated back into the project plan.

Name of Organisation	
Project Title / Change Description:	
Project Manager/ Lead details:	
Name of Data Protection Officer	
Date of Assessment:	

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project scoping. Summarise why you identified the need for a DPIA.
(See DPIA Procedure Step 1 for further guidance).

Step 2: Describe the Processing

2a Describe the nature of the processing:
(See DPIA Procedure Step 2 for further guidance)

How will you collect, use, store and delete data?

What is the source of the data?

Will you be sharing data with anyone?

What types of processing identified as likely high risk are involved?
Insert flow diagram showing data flows (optional)

2b Describe the scope of the processing:

(See DPIA Procedure Step 2 for further guidance)

Details of personal data

Please indicate what personal data will be collected/stored/processed, please indicate with an X where applicable.

Administration data

Name	☐
Date of Birth/Age	☐
Gender	☐
Contact details	☐
Unique identifier e.g. student number/NI No.	☐
Other data (please specify):	

Special Categories of data

Racial or ethnic origin	☐
Political opinion	☐
Religious or philosophical beliefs	☐
Trade Union membership	☐
Physical or mental health condition	☐
Sexual life and sexual orientation	☐
Genetic data	☐
Biometric data used to identify an individual	☐

Other sensitive information

Financial information/bank account details	☐
Criminal convictions and offences	☐
Other (please specify):	

Under Article 6 of the UK GDPR one of the following conditions needs to apply before the processing of personal data is lawful. Please indicate which condition applies: (See Appendix 2)

- The individual who the personal data is about has given/will give unambiguous consented to the processing ☐
- The processing is necessary for the performance of a contract with the individual ☐
- The processing is necessary for a legal obligation ☐
- The processing is necessary for the vital interests of someone (i.e. life or death situation) ☐
- The processing is carried out in the public interest or in the exercise of official authority ☐
- The processing is in the legitimate interests of the business or another party and does not prejudice the rights and freedoms of the individual (please provide further details): ☐

If processing Special Category Data, please state which of the conditions for processing specified in Appendix 2 applies.

2c Describe the context of the processing:

(See DPIA Procedure Step 2 for further guidance)

What is the nature of your relationship with the individuals?

How much control will they have?

Would they expect you to use their data in this way?

Do they include children or other vulnerable groups?

Are there prior concerns over this type of processing or security flaws?

Is it novel in any way?

What is the current state of technology in this area?

Are there any current issues of public concern that you should factor in?

Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

2d Describe the purposes of the processing:

(See DPIA Procedure Step 2 for further guidance)

What do you want to achieve?

What is the intended effect on individuals?

What are the benefits of the processing for you, and more broadly?

Step 3: Consultation

Consider how to consult with relevant stakeholders: (See DPIA Procedure Step 3 for further guidance)

Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.

Who else do you need to involve within your organisation?

Do you need to ask any relevant data processors to assist?

Do you plan to consult information security experts, or any other experts?

Step 4: Assess Necessity and Proportionality

Describe compliance and proportionality measures, in particular:
(See DPIA Procedure Step 4 for further guidance)

What is your lawful basis for processing?

Does the processing actually achieve your purpose?

Is there another way to achieve the same outcome?

How will you prevent function creep?

How will you ensure data quality and data minimisation?

What information will you give individuals?

How will you help to support their rights?

What measures do you take to ensure data processors comply?

How do you safeguard any international transfers?

Step 5: Identify and Assess Risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. (See DPIA Procedure Step 5 for further guidance and Risk Matrix)	Likelihood of Harm	Severity of Harm	Overall risk
Risk No. 01			
Risk No. 02			

Step 6: Identify Actions to Mitigate the Risks

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5 (See DPIA Procedure Step 6 for further guidance)
Add additional Risks as required

Risk	**Actions to reduce or eliminate risk**	**Effect on Risk** *(reduced / eliminated / Accepted)*	**Residual Risk** *(Low/ Medium/ High)*	**Action Approved** *(Yes/No)*
Risk No. 01				
Risk No. 02				

Step 7: Approval and Record of outcomes

(See DPIA Procedure Step 7 for further guidance)

Item	**Signed / Date**	**Notes**
Risk Actions approved by:		*Integrate actions back into project plan, with date and responsibility for completion*
Residual risks approved by:		*If accepting any residual high risk, consult the ICO before going ahead*
Consultation responses reviewed by:		*If your decision departs from individuals' views, you must explain your reasons*
DPO advice provided:		*DPO should advise on compliance, step 6 measures and whether processing can proceed*
Summary of DPO advice:		
DPO advice accepted or overruled by:		*If overruled, you must explain your reasons*
Comments:		
This DPIA will be kept under review by:		*The Data Protection Officer should also review ongoing compliance with DPIA*