

Data Protection Impact Assessment - template

Document Name	Enewsletter -DPIA
Author/Owner (name and job title)	Hannah Smith Senior Communications Officer (Digital)
Department/Team	Corp Communications
Document Status (draft, published or superseded)	Draft
Version Number	1.0
Release Date	
Approver (if applicable)	
Review Date	
Distribution (internal or external)	Internal

Welcome to the data protection impact assessment process. You should use this every time you want to implement or change a product or process. It is essential to managing your own project risks but also to managing the corporate risks of the ICO.

Responsibilities

It is your responsibility to ensure that data protection impact is taken into account during the design and build of your product or service. To do this successfully, you will need to be able to explain what your proposal is, and map out how data is used. This includes, amongst other things, where data might sit at any time geographically, but also the purpose of its use at different points in time.

Remember the basics. Key to a good assessment is knowing at all points in the process: what data you are collecting/using, why, where it will be stored and for how long, who will access it and why, how it will be kept secure and whether it's being transferred to any other country.

Your Information Asset Owner (your Director) is ultimately responsible for managing any residual risk once you have completed any mitigations to the risks you identify.

The Information Management Service, working on behalf of our DPO, can help complete the paperwork, provide compliance advice and spot risks. It is not the Service's responsibility to own, manage or mitigate the risks identified during the process.

Getting advice

You might also need advice from subject matter experts in other teams to make sure that you understand how something works or risks to what you are proposing to do. This is particularly likely if it involves new, or changing, technologies. Getting this advice will help to provide your IAO with assurance that you have understood and identified the risks.

You might well be working on a contract or agreement and a Security Opinion Report at the same time – these are also ways that you can mitigate risks and should be viewed as part of the overall assessment process.

The paperwork

You should think of this as a live document. You might change your plans or new information might come to light that changes the risk profile of your proposal. If that's the case, you should revisit the paperwork and update it to reflect any changes. You might also need to inform your IAO of new or changed risks.

The process

You should allow time for this process in your project plans. Start early! How long it takes will depend on what you're proposing, and how well you can explain it and identify risks. It can take several weeks to get the right advice and risk assessment in place.

Step 1

- Complete DPIA screening assessment. If you conclude that you do not need to complete a DPIA then you must make a record of your decision.
- If you do need to complete a DPIA then start completing the paperwork and notify the IM Service. Depending on what you're doing, the DPIA might need to be reviewed by the DPIA forum. You need to ensure the paperwork is sufficiently detailed, accurate and thorough before the forum is able to review it. This particularly applies to your descriptions of the processing activities you are proposing and how any associated technology works alongside it.
-

Step 2

- The forum is likely to provide advice and recommendations. You should consider this advice. If you decide not to follow it, then you must document your reasons why. If you do follow it, then most actions will need to be completed before go live. For example, updating privacy information or refining access controls.
- The forum is able to escalate risks to our Data Protection Officer and/or Risk and Governance Board if it is not comfortable with the processing activity being suggested or wants sign-off on advice.

When you have completed the DPIA paperwork and any actions, accepting that you might need to revisit it, you should get sign-off from your IAO before your product or service goes live.

If there are residual risks that your IAO would like to discuss, they can contact dpo@ico.org.uk. That discussion can be escalated to our Data Protection Officer and/or Risk and Governance Board if required.

Guidance for completing this template

Complete this Data Protection Impact Assessment (DPIA) template if your 'Screening Assessment - do I need to carry out a DPIA?' indicates a high risk to individuals. If you are unsure whether you need to complete a DPIA use the [screening assessment](#) first to help you decide.

Aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you will not be able to continue with your plans without changing them, or at all.

Guidance notes are included within the template to help you with its completion- just hover your mouse over any blue text for further information.

The [Information Management Service](#) is also available for further advice and support. Please keep in mind our [service standards](#) if you require advice.

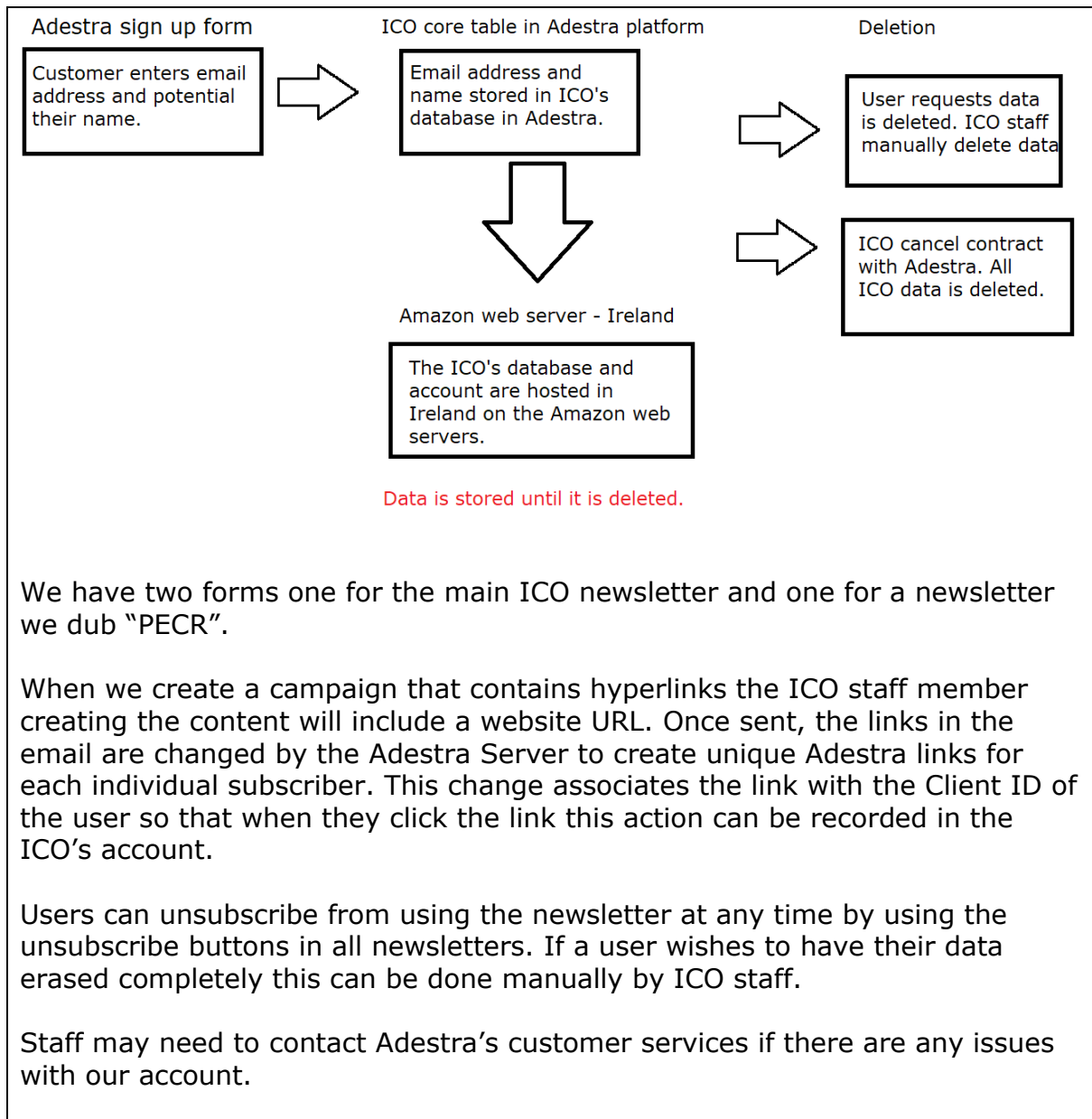
1. Process/system overview

1.1 Ownership

Project Title:	ICO Newsletter
Project Manager:	Hannah Smith
Information Asset Owner:	Director of Corporate Communications
Data controller(s)	ICO
Data processor(s)	Adestra – Upland Software Frost Bank Tower 401 Congress Avenue, Suite 1850 Austin, TX 78701-3788 833-UPLAND-1 (875-2631)

1.2 [Describe your new service or process](#)

Individuals sign up to receive email marketing messages from the ICO using a form hosted by Adestra.



1.3 [Personal data inventory - explain what personal data is involved](#)

Categories of data	Data subjects	Recipients	Overseas transfers	Retention period
<ul style="list-style-type: none"> • Contact profile including email addresses, client ID and names (optional) • Encoded URL string (including Client ID) • Analytics about clicks to links 	<p>Members of the public who have signed up to the newsletter.</p>	<p>Amazon Web Server (Ireland)(Sub-Processor)</p> <p>ICO</p> <p>Flairtech</p> <p>Adestra</p>	<p>Subscriber data is hosted in Ireland and is only available to ICO staff and Adestra support staff based in UK or Poland.</p>	<p>Information held in the contact profile of both subscribed and unsubscribed individuals will be held until the ICO stops sending email marketing via a direct marketing platform. It will only be hosted by Adestra until the ICO no longer has an account with them.</p> <p>The encoded links are not stored by Adestra or the ICO. They exist only on the email sent to the individual.</p> <p>Analytics data is deleted from an individual’s contact profile after 24 months.</p> <p>Analytics data about clicks remain associated with campaign for 24 months after the event has happened.</p>

<ul style="list-style-type: none"> Staff emails and name. 	Staff with Adestra logins and who email Adestra customer services	Adestra FlairTech (sub-processor)	<p>Staff login information is stored on the ICO Adestra account and on the Amazon Web Servers.</p> <p>Staff information may be sent to customer service offices in the UK or Poland.</p>	<p>Staff account information is deleted when they no longer need the log in ie they change roles, move departments or leave the organisation.</p> <p>This is not retained by Adestra/Flairtech indefinitely or till such time they are asked to be deleted. The ICO will request our emails be deleted once our contract with Adestra ends.</p>

1.4 [Identify a lawful basis for your processing](#)

Opt in consent is required to comply with PECR.

The lawful basis we rely on for processing contact profile data including mandatory collection of email addresses and optional collection of names is your consent under article 6(1)(a) of the GDPR

The lawful basis we rely on for processing of staff information is article 6(1)(b) – contract.

The lawful basis we rely on for processing of analytics information is article 6(1)(e) – public task.

1.5 [Explain why it is necessary to process this personal data](#)

We use email addresses to send subscribers our E-newsletter. We cannot send the newsletter without this information. The newsletter is a key way for us to communicate important information about our work and the law with stakeholders. We ask for names in case we send personalised newsletters, this is not essential so we have made it optional.

We use the encoded URL string to record what links have been clicked by which client ID. Having the overall number of clicks to a link helps us to record the impact, awareness and engagement of areas of our work and the law, which helps many areas of the business with their planning and reporting. We have reduced the intrusiveness of this practice as we do not use any tracking technology or technology that accesses users devices.

We are also able to use the information about previously clicked on links to send information to smaller groups of subscribers based on their previous interests This helps the ICO deliver more targeted communications, improving the effectiveness of our comms work. It will benefit the user as it ensures they receive information tailored to their interests or stops them receiving too many irrelevant emails from the ICO. All the information sent out in the newsletter is available on other ICO channels such as the website and social media so no one is excluded from accessing information or events due to this use of filters.

Staff are not asked to share any personal data with the customer service team other than their work email and name. It is essential that staff contact the customer services team to keep the newsletter service working efficiently and effectively. This activity is within the reasonable expectation of staff.

1.6 [Outline your approach to completing this DPIA](#)

We have consulted with Adestra about the use of technologies and overseas transfers.

We have consulted with [Tech Policy](#). Below is a summary of their advice:

- Adestra does not appear from the information provided to engage Reg.6 of PECR to the extent that it does not access or store information on terminal equipment.
- You may wish to reconsider the privacy notice changes to ensure you properly reflect the processing taking place and the appropriate lawful basis relied upon,
- You may wish to assess Adestra's features against our AI guidance,
- You may also wish to carry out a DPIA, if you haven't already.

We have consulted with Information Management for advice on Data Protection concerns.

We've consulted with Cyber Security.

We will not consult with the public. The newsletter has been established at the ICO for over a decade and there is very limited use of personal data. Sending email marketing is a common practice. For these reasons, it may seem strange to subscribers to consult with them at this point about this processing.

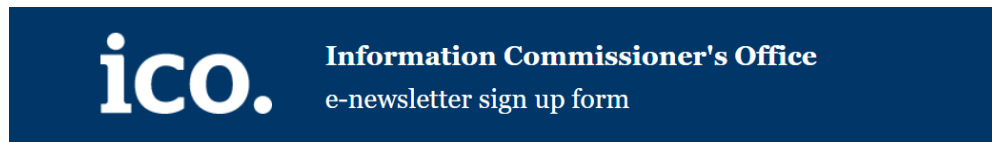
2.0 Data flows

2.1 Provide a [systematic description of your processing](#), from the point that the data is first collected through to its destruction. If your plans involve the use of new technology you should explain how this technology works and outline any 'privacy friendly' features that are available.

Individuals sign up to receive email marketing messages from the ICO using a form hosted by Adestra. They sign up by giving us their email address (mandatory) and name (optional).

We have two forms one for the main ICO newsletter and one for a newsletter we dub "PECR". These are linked to from the ICO's website.

The forms are identical and say the following (accurate as of 21 June 2021):



* denotes a mandatory field


First name

Last name

Email *

We use a third party provider, Adestra, to deliver our monthly e-newsletter. We gather statistics around email opening and clicks using industry standard technologies including clear gifs to help us monitor and improve our e-newsletter.
For more information, please see our [privacy notice](#).

Are you human?



The data of everyone who has subscribed to any ICO newsletter at any time is stored in the ICO's core table.

Each contact profile is associated with "lists" that allow us to know which newsletters they could be receiving.

We have four main lists, two associated with the main newsletter and two associated with "PECR" newsletter. Each newsletter has a main list and an extras list.

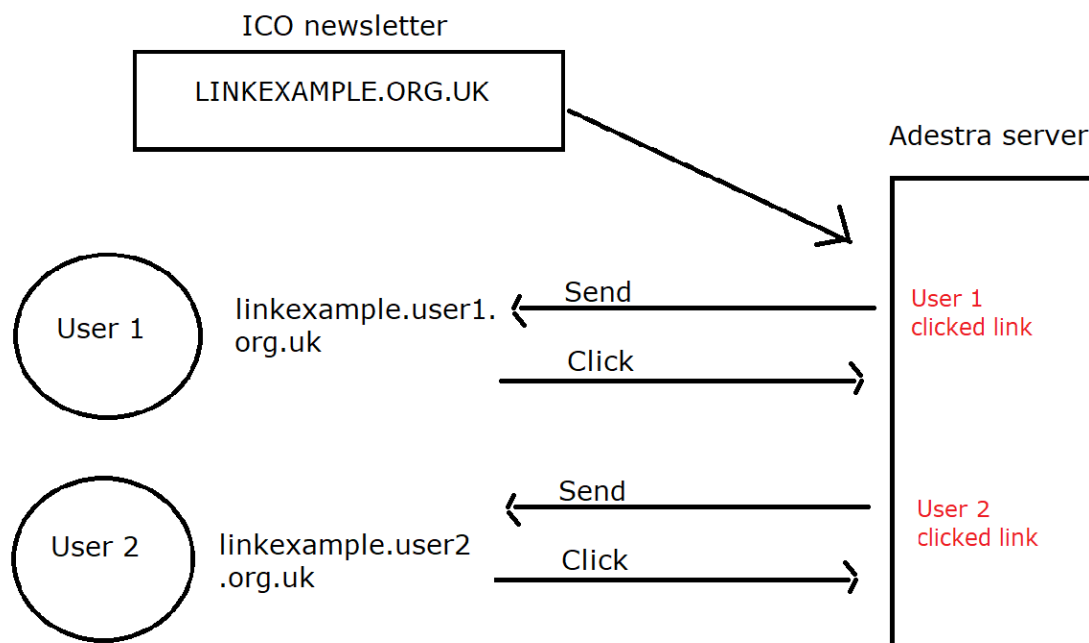
The main list contains the information of people who have only signed up to receive monthly updates. This is what the privacy notice said at the time they subscribed. Their consent is still valid as they consented to receiving a monthly email from the ICO and have not indicated they no longer wish to receive this. But they **must not** receive more than one email a month.

We have now changed the privacy statement to say we send updates “at least once a month”. Anyone who signed up after this time is put on both the monthly newsletter list and another list called “extras” so we know who has consented to receive more than one email a month.

When we create an email or “campaign” we select which list to send it to and only the people on that list will receive it.

Data collected prior to 2018 was done so either through Adestra as described above.

When we create a campaign that contains hyperlinks the ICO staff member creating the content will include a website URL. Once sent, the links in the email are changed by the Adestra Server to create unique Adestra links for each individual subscriber. This change associates the link with Client ID of the user so that when they click the link this action can be recorded in the ICO’s account. The data (link click) is collected for the ICO’s use **only** and is for analytics purposes or to customise ICO lists.



Adestra have said in respect of their patented link tracking technology:

“The link tracking system does not use any technology (localstorage, cookies, etc) to store or access data on the user’s device.”

ICO Technology Policy department have advised:

"Adestra does not appear from the information provided to engage Reg.6 of PECR to the extent that it does not access or store information on terminal equipment.

The patent goes into indepth information as to how the encoding of the URL strings is carried out, the Adestra solution use of encoded URL strings permits the unique identification conversions of individual users to specific links by virtue of the **contact_ID** and **campaign_ID** fields respectfully. This would permit further granular processing of individual than simple click tracking (+1 cumulative visits). It appears that these URL strings would meet the definition of personal data under Art.4(1) UK GDPR. The encoding, and storage of the **contact_ID** and subsequent processing of these URLs in the event records/reports also appear to meet the definition of pseudonymous processing under Art.4(5).

As such, my previous advice regarding completion of a DPIA and correctly reflecting the processing in the privacy notice(s) etc. remains. Likewise, my advice in relation to machine learning/ICO AI guidance (in so far as these offerings by the Adestra solution are being deployed) still stands"

The ICO is able to create customised lists based on the actions taken by users in the past. For example, if we were sending a campaign that focussed solely on guidance for SMEs, we could narrow down our large list of subscribers by creating rules that filters the list down by users who have clicked on links to SME guidance in the past. This helps us ensure we are sending relevant information to the right people. This is done manually and does not use Algorithms, ML or AI and therefore Article 22 does not apply.

The ICO does not utilise any Adestra products or functions that use AI or ML to process ICO data.

If a user forwards the newsletter on to a third party the ICO will not have access to any personal information about the third party. If the third party clicks on a link from the newsletter this will be recorded as a click by the original recipient. This could mean the original recipient could receive targeted emails from the ICO based on inaccurate data.

Users can unsubscribe from receiving the newsletter at any time by using the unsubscribe buttons found in all newsletters. Their contact profile is not deleted but moved to an unsubscribe list, which works as a filter to ensure they do not receive newsletters from the ICO. We are also able to move users to this list automatically if requested or delete their data from all lists including the unsubscribe.

Information held in the contact profile of both subscribed and unsubscribed individuals will be held until the ICO stops sending email marketing via a direct marketing platform. It is important that email addresses are stored even after

a user has unsubscribed as users are able to make multiple contact profiles with the same email address but when they unsubscribe only one of these contact profiles will be moved to the unsubscribe list. However, the unsubscribe list works as a filter and will not allowed the duplicate contact profiles with the same email address to be sent the campaign.

[Direct marketing guidance](#) from the ICO in 2016 states:

“Organisations should maintain a ‘suppression list’ of people who have opted out or otherwise told that organisation directly that they do not want to receive marketing.”

We can permanently delete a contact profile of a subscribed or unsubscribed user at any time.

Analytics are recorded about users in two ways. Some information is associated with their contact profile and some information is associated with the campaign. Analytics associated with the individuals contact profile are deleted after 24 months automatically. When a user unsubscribes the analytics data associated with their email address is not automatically deleted – it will remain associated with their email address for 24 months – in line with the retention. In order to delete the data before then – we need to delete the user from the system entirely. This is not done as a matter of course but can be done if a user puts in a request. Analytics data about clicks remains associated with campaigns for 24 months after the event has taken place (not 24 months after the campaign is launched). For example, if in September 2021 a user clicks a link from a campaign launched in September 2018 the analytics data will remain associated with the campaign until September 2023.

If a user forwards the email to another email address (whether they are subscribed themselves or not) – if the recipient of the forwarded email clicks a link – Adestra will record this against the original recipients email address.

The Adestra servers that host the ICO’s data are based in Ireland they use a Amazon Web Servers as a sub-processor for this activity.

Adestra also use FlairTech based in the UK and Poland to manage their customer services. When a ticket is raised by the ICO about issues relating to our account the staff email will be sent to the sub-processor. The staff at Flairtech are able – with ICO permission – to access our data. However, it remains within the ICO’s account and isn’t moved or processed elsewhere. The support service have informed me that enquiries are kept indefinitely unless they are requested to delete them.

3.0 [Key principles and requirements](#)

[Purpose & Transparency](#)

1. Will you need to update our [privacy notices](#)?

Yes No

2. If you are not updating our privacy notices how do you intend to communicate information about your processing to the data subjects?

NA

3. If [consent](#) is your lawful basis for processing personal data are you maintaining appropriate records of the data subjects consent?

Yes No N/a

4. If legitimate interests is your lawful basis for processing have you completed a [legitimate interest assessment](#)?

Yes No N/a

If applicable please provide a link to your completed assessment.

Accuracy

5. Are you satisfied the personal data you are processing is accurate?

Yes No

6. How will you ensure the personal data remains accurate for the duration of your processing?

If email addresses become out of date Adestra will get a bounce back when we send a campaign. If the they get three bounces, the email is moved to the suppression list to ensure only working email addresses are on the list.

7. If the personal data isn't being obtained directly from the data subject what steps will you take to [verify accuracy](#)?

n/a

Minimisation, Retention & Deletion

8. Have you done everything you can to minimise the personal data you are processing?

Yes No

9. How will you ensure the personal data are deleted at the end of the retention period?

In relation to the analytics data related to contact profiles – this is deleted automatically by Adestra. This can be checked via the ICO’s account.

Adestra is contracted to delete the ICO’s data after delete our account.

The ICO will request our enquiries are all deleted when our contract with Adestra ends.

10. Will you need to update the [retention and disposal schedule](#)?

Yes No

Integrity and confidentiality

11. Where will the personal data be [stored](#)?

The personal data is stored on the ICO’s Adestra Account, which is accessible by limited ICO personnel through password and 2AF accounts.

It is stored on Adestra servers in the UK.

12. Are there appropriate [access controls](#) to keep the personal data secure?

Yes No

13. Have you contacted the [cyber security team](#) for a security assessment of your plans?

Yes No N/a

If applicable please provide a link to any assessment.

14. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

All Comms staff are trained how to use the Adestra account before they are able to send campaigns.

New processes will be put in place in relation to the deletion of old campaigns.

The Senior Comms Officer responsible for managing the admin of the account ensures all new users are issued with passwords and OTPs.

Accountability

15. Who will be the [Information Asset Owner](#) for this personal data?

Director of Communications

16. Will you need to update our [Article 30 record of processing activities](#)?

Yes No

17. If you are using a data processor have you agreed, or will you be agreeing, a written contract with them?

Yes No N/a

Individual Rights

18. Is there a means of providing the data subjects with [access](#) to the personal data being processed?

Yes No

19. Can [inaccurate or incomplete](#) personal data be updated on receipt of a request from a data subject?

Yes No

20. Can we [restrict](#) our processing of the personal data on receipt of a request from a data subject?

Yes No

21. Can we [stop](#) our processing of the personal data on receipt of a request from a data subject?

Yes No N/a

22. Can we [extract and transmit](#) the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes No N/a

23. Can we [erase](#) the personal data on receipt of a request from the data subject?

Yes No

Risk Description	Response to Risk	Risk Mitigation	Expected Risk Score		
			I	P	Total
			See Appendix 1 – Risk Assessment Criteria		
Access controls are not implemented correctly and personal data is accessible to an unauthorised third party.	Reduce	<p>The Senior Communications Officers (digital) has is responsible for managing the user access and authorising new access.</p> <p>Only communications staff and business development staff have access to the account.</p> <p>People are only given full access rights if they require them to manage user admin (senior comms officers) or because they need access to all areas for technical reasons (business development staff). All other staff have limited access, which means they are unable to edit or delete user data, they cannot bulk export data and they cannot give users access to the account.</p> <p>We will ensure passwords and 2FA are enabled on all accounts.</p> <p>There is minimal data stored on the system and no SCD.</p>	2	2	4-low

Human error – sending a campaign to the wrong list.	Reduce	<p>There are different workspaces for different newsletters – so someone signed up to “PECR” couldn’t accidentally be sent the standard newsletter.</p> <p>Users must enter their password before launching a campaign.</p> <p>Staff are trained before sending newsletter so know which lists are which.</p> <p>Adestra can stop campaigns for sending once launched. However, if someone on the list has already received the email that cannot be undone.</p>	1	1	<p>1- low</p> <p>This is more of a reputational risk than a risk to individuals as sending to the wrong list is a breach of PECR.</p>
Adestra experiences a data breach and ICO data is lost/stolen	Reduce	<p>We have ensured ICO data is only stored on servers in the EEA.</p> <p>Cyber Sec undertook a security assessment when Adestra were procured.</p>	2	1	2 - Low
People believe that by unsubscribing they are enacting right to erasure not realising their data continues to be held by the ICO.	Reduce	Make this very clear in the privacy notice.	1	2	2 -low
Individuals risk losing the protection of the UK GDPR as their personal		The transfer of data is from the UK to the EEA only. The GDPR is considered	1	1	1 - low

data is transferred outside of the UK.	Accept	adequate by the UK Government and therefore provides adequate protection to individuals' data. The data being transferred is minimal and contains no SCD.			
Data is inaccurate due to subscribers forwarding on emails to others and having that person's behavior recorded on their client record.	Accept	The person has signed up to receive information from the ICO so they would not receive any information they haven't consented to receive – even if some of it is of less interest than others due to being targeted based on other people's behaviour. In the future it may be possible to have preference centres that people opt in to so that link clicks do not determine who receives what.	1	1	1 -low
Use of data collected before GDPR without additional consent.	Reduce	Renew consent	2	5	10 - med (this score reflects the risk to individuals of continuing to use data collected without refreshing consent – see 7.0 below)
Accuracy – a user may receive a targeted email based on inaccurate	Reduce (present)_	All targeted email are about the work of the ICO. People who sign up to receive the	2	2	4 - low

<p>data if they forward an email to a third party.</p>	<p>Avoid (future)</p>	<p>newsletter have requested to hear about the work of the ICO. If they receive a targeted email it may not be totally relevant to their area of interest but it is still relevant to what they signed up to receive.</p> <p>In the future, we intend to set up preference centres which allow users to select their areas of interest rather than relying on past behaviour. This would eliminate this issue.</p>			
--	-----------------------	--	--	--	--

4.0 [Risk assessment](#)

5.0 Consult the DPO

Guidance: Submit your DPIA for consideration by the DPIA Forum. The process to follow is [here](#). Any recommendations from the DPOs team will be documented below and your DPIA will be returned to you. You should then record your response to each recommendation.

	<u>Recommendation</u>	<u>Date and project stage</u>	<u>Project Team Response</u>
1.	The duplicated diagram showing the hyperlink process in 1.2 isn't necessary and can be removed. We recommend you replace it with a high level diagram that shows the data flow from customer sign up and covers storage and deletion.	08/07/2021	Accept
2.	It's not clear how long analytics data is kept after somebody opts out as there are references to both 12 and 24 months. Equally it's not clear if this remains linked to the individual or campaign only. Please clarify and update.	08/07/2021	Accept
3.	There's no mention of the personal data required to provide logins to ICO staff. This should be incorporated into your data inventory at 1.3.	08/07/2021	Accept
4.	Review and update both the privacy notice and the description of what our e-newsletter is to improve transparency of processing and	08/07/2021	Accept

	better inform customers about what they can expect in terms of content and frequency of contact.		
5.	We've updated section 1.4 but we're requesting advice from policy teams regarding the decisions made regarding lawful basis. Iman Elmehdawy to provide a separate communication to Hannah Smith to confirm outcome.	08/07/2021	Accept
6.	Refresh consents once privacy notice and description of e-newsletter have been updated.	08/07/2021	Partially accept. We will look into and action something to refresh consent but we will not do this before the next enewsletter is released.
7.	Clarify what would happen if somebody received the newsletter e.g. a DPO and then forwarded to colleagues who then clicked links? How would this affect the accuracy of the contact profile and the customised lists being created. Add content into DPIA.	08/07/2021	Accept
8.	More information required in DPIA about the origin of the old lists – when and how were these created, are these stored solely with Adestra or do they exist in other places (Excel, ICE etc.)?	08/07/2021	Accept
9.	The Legitimate Interest Assessment states that you can't offer an opt out. This would indicate that legitimate interests isn't the correct lawful basis for processing analytics data. Please clarify and amend.	08/07/2021	Accept

10.	The legitimate interests assessment refers to staff data but the lawful basis for processing this data is contract so these references should be removed from the LIA.	08/07/2021	Accept
11.	An operational procedure for the newsletter is drafted which establishes responsibilities and processes for managing deletion at the end of the retention periods, the granting and review of access permissions including the deletion of old accounts when staff leave or change roles.	08/07/2021	Accept
12.	There's a risk retention and disposal rules aren't actioned since deletion is being diarised by one individual. This should be added to the Risk Assessment. Operational procedure (above) and a process of peer review and/or diarising in a team calendar rather than individual calendar should be considered as mitigation.	08/07/2021	Accept
13.	Risk Assessment states "We have ensured ICO data is only stored on servers in the UK.". This may be an inaccurate statement as DPIA also indicates help desk in Poland and subscriber data is transferred to Ireland. Clarify and amend.	08/07/2021	Accept
14.	Remove statement that "Minimal data is stored on the system and no	08/07/2021	Accept

	SCD.". Recommend removing as whilst data is minimal per data subject collectively this is a large dataset and a breach would affect a large number of individuals.		
15.	The use of old contact lists is a risk so recommend this is added to the risk assessment.	08/07/2021	Accept

6.0 Integrate the outcomes back into your plans

Guidance: Identify who is responsible for integrating the DPIA outcomes. The outcomes include any expected mitigation you need to take as identified in your risk assessment and any further actions resulting from the DPOs recommendations.

Action	Date for completion	Responsibility for Action	Completed Date
Update DPIA to reflect points 1,2,3,7,8 and 14 above	20 July 2021	Hannah Smith	
Write and amend both privacy notices	1 August 2021	Hannah Smith	
Send information to HS regarding decisions on lawful basis.	21 July 2021	Iman Elmehdawy	
Create plan for renewal of consent	1 September 2021	Hannah Smith	
Undertake renewal of consent exercise	31 March 2022	Hannah Smith	
Change lawful basis for analytics data to public task (after policy advice)	20 July 2021	Hannah Smith	
Change lawful basis for staff data to contract (after policy advice)	22 July 2021	Hannah Smith	

Write an operational procedure document	5 August	Hannah Smith	
Diarise the deletion dates in public diary	5 August	Katie Makepeace-Warne	
Add risk of human error in relation to deletion of data to risk assessment	20 July 2021	Hannah Smith	

7.0 Expected residual risk and sign off

Guidance: Summarise the expected residual risk below. This is any remaining risk *after* you implement all of your mitigation measures and complete all actions.

It is never possible to remove all risk so this section shouldn't be omitted or blank. If the expected residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO as the regulator by following the process used by external organisations.

The expected risk score is low for all identified risks with one exception.

The ICO is using data it collected before the implementation of the GDPR and has not sought to renew the consent. The privacy notice requires an update to ensure data subjects are fully informed about the processing so their opt in consent remains valid.

Although the impact to individuals is low, continuing to rely on old consents means the probability score for this risk is high, giving an expected medium risk level.

The renewal of consent cannot take place before the next newsletter is sent so residual risk remains medium until this activity can take place.

We will continue to keep the old contacts off the "new" list until we have sought renewal of the consent. Once the privacy notice is updated and renewal of consent has taken place the residual risk should be low for all identified risks.

7.1 IAO sign off

IAO (name and role)	Date	Project Stage
Angela Balakrishnan – Director of Corporate Communications	02/08/2021	Complete.

8.0 [Change history](#)

Guidance: To be completed by the person responsible for completing the DPIA and delivering the system, service or process)

Version	Date	Author	Change description
V0.1	June 2021	Hannah Smith	First Draft
V0.1	08/07/2021	Steven Johnston	Recommendations from DPIA forum added to 5.0.
V0.2	22/07/2021	Hannah Smith	Clarification and adjusts made to address DPIA forum recommendations. Two additional risks added to list. Actions included in action plan.
V0.3	29/07/2021	Steven Johnston	Amends made to risk about re consent
V0.4	02/08/2021	Angela Balakrishnan	Sign off.
V0.5	18/08/2021	Hannah Smith	Changes made to information about retention of analytics data associated with campaigns after receiving clarity from Adestra.

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).

Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability

Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level

Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability \ Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high	Amber	Amber	Red	Red	Red

(5)	(5)	(10)	(15)	(20)	(25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria

These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: example risks to data subjects

Guidance: The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider specific risks that are relevant to your plans.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects
- Excessive data is processed
- Data is not kept up to date
- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights

- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises
- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions
- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)
- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the data controller (employee/employer)
- Source of data poses risks re accuracy (obtained from a unverified or old list)
- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g. fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behavior
- Non-compliance with DP principles

9.0 Template Change History (for Information Management Service only)

Version	Date	Author	Change description
v0.1	01/06/2020	Steven Johnston	First draft
v1.0	07/10/2020	Steven Johnston	First release
v1.1	07/01/2021	Iman Elmehdawy	Amendment to guidance note page 2.
v.1.2	18/03/2021	Helen Ward	Addition of Privacy by design at the ICO (pages 2 and 3)