DPIA

Project: Phase 1 New Website

Completed by: Head of Policy and Information/ Acting Head of Policy and Information

Review frequency: 2 years (or as required)

Next review date: March 2024

Contents

Part A: Project overview

No.	Question	Response	Comments/notes
1	Explain the aims of the project, the anticipated benefits to the organisation, to individuals and to other parties.	A new phase 1 website (Phase 1 website) is being developed for the Scottish Information Commissioner, since the current website is being decommissioned. The Scottish Information Commissioner (the Commissioner) requires a website in order to effectively meet and deliver their statutory duties (including compliance with FOI law). A website is also required in order to provide information to public authorities and members of the public about FOI, and their duties and rights. The Phase 1 website project will involve development, build and launch of a new website for the Commissioner, and ongoing maintenance and hosting of this website. A contract for the development and build of the Phase 1 website was awarded on 5 January 2022 and this included relevant UK GDPR and data protection provisions. The Phase 1 website is expected to go live by 7 April 2022. The benefits of the Phase 1 website include: - Increased effectiveness of main channel for circulation of detail about FOI law, duties and rights - Reaching increased audience via more effective website - It is anticipated that the project will increase internal skills, confidence and literacy on website and digital matters within the Commissioner's office, enabling higher confidence and quality work in this area to take place in future. - Ensuring Commissioner's web presence is secure, accessible and fit for purpose - Ensuring compliance with relevant standards and statutory/regulatory requirements - Decrease in time required for staff to edit and upload documents and information to the website - Data minimisation – new website is stripped of all functionality that raised UK GDPR and data protection concerns – personal data is limited and only published/processed where required or necessary.	
2	Describe the personal information	Data type 1: Names and email addresses of staff acting as website administrators. These will not be available publicly – only accessible by the Commissioner's staff and website	

	affected in terms of data sets.	contractor. Data type 2: Names, job titles, diaries, biography details, signatures and registers of interests (Senior Management Team (SMT), members of the Advisory Audit Board and the Commissioner), SMT attendance at external meetings, minutes of SMT meetings and some limited instances of names of external speakers at events, on relevant pages of the website. These will be available publicly to people browsing the relevant website pages. Data type 3: Photo of the Commissioner, used to illustrate a limited number of pages on the website. These will be available publicly to people browsing the relevant website pages. Data type 4: Website analytics – although Anonymize IP is installed this is only available to the Commissioner's staff, website contractor and Google Analytics. We are soon to move from Universal Google Analytics to GA4, which will not store any IP addresses, thus reducing any privacy concerns further.	
3	Are any of these data sets considered to be high risk? If so, why?	FOR DATA SETS 1-4 No. None of the personal data capture falls within the definition of special category data.	
4	Describe the proposed collection, use and deletion of personal information and identify the relevant data controllers and data processors involved. It may be useful to refer to a flow diagram or another way of explaining the data flows.	FOR DATA TYPE 1 (Staff web admin details): • Collection: Data added and edited by the Commissioner's staff and website contractor, The Union. • Use: This will be used to create and provide access for relevant staff to administer the Commissioner's website. This includes creating and editing webpages, and uploading documents or files. • Data controller: Scottish Information Commissioner • Data processor: Website hosting and support contractor. At present, access is limited to those who require access for their jobs or for business resilience reasons (the SMT). In due course, and when finalised, the protocol is due to be approved by SMT (the intended protocol is not likely to differ to any great extent from the protocol that was in place for the previous website). FOR DATA TYPE 2 (Details of staff and event speakers on web pages): • Collection: Staff details will be added as relevant to required pages, generally by	

		staff who administer the website, and with the knowledge of the relevant staff. Names of speakers at events are listed in relevant news items if required, and where in the public domain. • Use: Staff details will be included to set out who is in the Commissioner's team, to note author of reports/articles, or to describe relevant management activities (in reports, minutes, updates or diary listings). Names of speakers at events are listed in relevant news items if required to promote the event or to make it clear who is participating, and where in the public domain. • Data controller: Scottish Information Commissioner • Data processor: Website hosting and support contractor. <u>FOR DATA TYPE 3 (Commissioner's photo):</u> • Collection: Images used from Commissioner's image library. • Use: These will be used to illustrate a limited number of relevant pages – for example the 'About the Commissioner' page and Contact us / enquiries section on the homepage. • Data controller: Scottish Information Commissioner • Data processor: Website hosting and support contractor. <u>FOR DATA TYPE 4 (Website analytics):</u> • Collection: We will use a third party service, Google Analytics, to collect details of website visitor behaviour patterns. To do this, Google Analytics uses online identifiers, cookie identifiers, IP addresses (though without the last three digits, as 'AnonymizeIP' feature is in place) and device identifiers. Our cookie tool allows users to manage these cookies. Our cookie tool is being tested during user acceptance testing in June 2022. • We are soon to move from Universal Google Analytics to GA4, which will not store any IP addresses, thus reducing any privacy concerns further. • Use: These will be used to monitor numbers of visitors to different parts of the Commissioner's website so updates can be planned and progress toward targets monitored. The information will not used to identify anyone. • Data controller: Scottish Information Commissioner • Data processor: Google Analytics and website contractor.	

At present, access is limited to those who require access for their jobs or for business resilience reasons (the SMT). In due course, and when finalised, the protocol is due to be approved by SMT (the intended protocol is not likely to differ to any great extent from the protocol that was in place for the previous website).

5	Is the information obtained from the individual data subjects, themselves or from third party sources? Provide details.	FOR DATA TYPE 1 (Staff web admin details): Provided on behalf of staff by administrator, in same organisation. FOR DATA TYPE 2 (Details of staff and events speakers on web pages): Data for staff entered by staff, and event speakers' names entered by Commissioner's staff, taken from third party sources (publicly available only). FOR DATA TYPE 3 (Commissioner photo): Photos were taken with Commissioner's knowledge, and are stored on the website and on the Commissioner's IT systems. FOR DATA TYPE 4 (Website analytics): Collected by third party (Google Analytics), generated by activity of individual subjects.	
6	Describe why it is necessary to process personal information for this project. Explain the purposes for which the personal information will be processed.	FOR DATA TYPE 1 (Staff web admin details): Required in order for staff to be able to edit and administer the website, so accounts for them can exist and so they can perform their duties. FOR DATA TYPE 2 (Details of staff and events speakers on web pages): Required to provide transparency regarding the Commissioner's organisation, and to promote attendance at relevant events. FOR DATA TYPE 3 (Staff photos): To provide a visual representation of the Commissioner. FOR DATA TYPE 4 (Website analytics): To monitor performance of the website, progress towards targets, and plan improvements and updates.	
7	On what legal basis will you rely to process the information?	FOR DATA TYPE 1 (Staff web admin details): **Contractual necessity** (for performance of contract of employment – not all members of staff will be website administrators) FOR DATA TYPE 2 (Names of staff and events speakers on web pages): **Contractual necessity** (for performance of contract of employment) for staff details; **Public interest task** - exercise of Commissioner's statutory functions for event details. FOR DATA TYPE 3 (Commissioner photo): **Consent**	Please see Processing Conditions Guidelines.

		FOR DATA TYPE 4 (Website analytics): **Consent** – managed through cookies tool on website. Consent refreshed during each user session. Will not be required when we move to GA4 (see above).	
8	If applicable, on what legal basis will you rely to process a special category of personal information?	NOT APPLICABLE	Please see Processing Conditions Guidelines.
9	If you are relying on consent/explicit consent, do you have an appropriate procedure in place for: □ Obtaining and recording in an auditable way that consent has been given?; □ Stopping any processing based on that consent and, if necessary, deleting the personal data provided in the event that the data subject indicates that they are withdrawing consent?	FOR DATA TYPE 3: Yes Obtaining and recording: Where photos are taken, this is done with use of relevant consent form and following guidance and procedures set out in the Commissioner's Data Protection Policy and Handbook. Stopping processing / deleting: Ensuring files are stored appropriately so they can easily be found and deleted as required.	

10	Do you believe that the SIC's current privacy notice gives sufficient information to affected individuals about the processing that will be conducted?	FOR DATA TYPE 1 (Staff web admin details): Yes – see 'working for us' section FOR DATA TYPE 2 (Details of staff and events speakers on web pages): For staff yes – see 'working for us' section; for event speakers, nothing specific is included. FOR DATA TYPE 3 (Staff photos): Yes – see 'working for us' section FOR DATA TYPE 4 (Website analytics): Yes – see 'Visiting our website' section (updated in line with what is stated above)	*Existing privacy notice sufficient subject to amendment to Google Analytics – cookie tool now allows user to opt in to using cookies.*
11	Which stakeholders, individual data subjects or representatives (if any) should be consulted, internally and externally? How will you carry out the consultation? This should be linked to the relevant stages of the project management process. Consultation can be used at any stage of the DPIA process.	• The website will be used in order to support the work of Commissioner. • The Policy and Information Department manage the Phase 1 website contract (and manage the ongoing support and maintenance contract). • the Enforcement Department use and upload decisions to the website • the Corporate Services Department upload and maintain the corporate information which includes: About Us, Publication Scheme and the Commissioner's Guide to Information, SMT meeting agendas, papers and minutes, and other key corporate areas. • The Heads of department will be involved and consulted in any action. • The GDPR Working party will consider the draft DPIA • The DPO will be consulted on the draft DPIA • The DPIA will be document subject to regular review throughout the remaining timeframe of the Phase 1 website The SMT will consider the DPIA and make decisions on any actions required.	
12	Is it possible for individuals to	Not generally. Yes – Commissioner can refuse consent for photo/s.	

	restrict the purposes for which the Commissioner will process the personal information?		
13	Are decisions being made on the basis of the personal information that will be processed?	No	
14	If the answer to 13 is yes, will these decisions have legal or significant effect on the individuals concerned?	N/A	
15	Is the processing by automated means?	No	*There are specific provisions that apply to automated processing. These should be considered if the answer to this question is yes.*
16	Are procedures in place to provide individuals access to personal information about themselves?	Yes, in line with existing procedures on subject access requests. In addition: • FOR DATA TYPE 1, subjects may log in and view/edit their own details, • FOR DATA TYPES 2 and 3 the data is publicly available on the Commissioner's website and so may be accessed there. • DATA TYPE 4 – Anonymize IP in place.	*Consider the sufficiency of resources, IT and technology used in the project to ensure compliance with data protection obligations to*

			allow data subject to access personal information about themselves.
17	Can the personal information be corrected by the individuals, or can individuals ask for correction of the information.	Yes, in line with existing procedures and as set out in privacy notice, for data types 1 – 3. In addition, for data type 1, subjects may log in and edit their own details, and for remaining data types, the subject can ask for correction via email or any other contact route. For data type 4, this cannot be conducted as individuals cannot be identified (as a result of use of AnonymizeIP).	
18	Do you check the accuracy and completeness of personal information on entry?	FOR DATA TYPE 1 (Staff web admin details): Yes, following account set up, to ensure website administration functions work correctly. FOR DATA TYPE 2 (Details of staff and events speakers on web pages): Yes, following key document procedures where appropriate. FOR DATA TYPE 3 (Staff photo): - Yes - consent FOR DATA TYPE 4 (Website analytics): n/a	
19	How often will the personal information you process be updated?	FOR DATA TYPE 1 (Staff web admin details): Ad hoc – when staff change details or leave employment. FOR DATA TYPE 2 (Details of staff or event speakers): Ad hoc - when relevant entries are updated as part of ongoing maintenance and reviews, or speakers change (or at required intervals where details are contained in key documents, which have regular review periods specific to the individual documents or ad hoc reviews carried out). FOR DATA TYPE 3 (Staff photos): Ad hoc - when website page illustrations change or are removed due to requirements arising or regular maintenance and reviews. FOR DATA TYPE 4 (Website analytics): Ongoing process, information is continually refreshed.	
20	How severe	FOR DATA TYPE 1 (Staff web admin details): Some (but very limited) consequences, as	

	would you deem the consequences, in case you process outdated personal information for the individuals it refers to?	would restrict ability to conduct duties, but issue would be easily identified and rectified. FOR DATA TYPE 2 (Details of staff and events speakers on web pages): Some (but limited) consequences, as may temporarily mislead public regarding details of Commissioner or staff, or speakers at events; but issue would be easily identified and rectified. FOR DATA TYPE 3 (Staff photo): Not severe, as images illustrative only. Photos will be removed/updated in line with staff/Commissioner changes. FOR DATA TYPE 4 (Website analytics): Not severe, as data not used to or sufficient to identify individuals (given AnonymizeIP function active).	
21	Which measures and/or procedures will be adopted as a safeguard or security measure to ensure the protection of personal information?	FOR DATA TYPE 1 (Staff web admin details): Website content and security safeguards provided by website contractor; access restricted to relevant staff only (see reference to proposed protocol in section 4 above) FOR DATA TYPE 2 (Details of staff and events speakers on web pages): Only required data used, stored and made available; website content and security safeguards provided by website contractor. Content can only be uploaded or updated on the website by website administrators, who have required level of access; accounts are password protected. FOR DATA TYPE 3 (Staff photo): Only required photos used, stored and made available; website content and security safeguards provided by website contractor. Content can only be uploaded or updated on the website by website administrators, who have required level of access; accounts are password protected. FOR DATA TYPE 4 (Website analytics): AnonymizeIP feature activated to ensure no users identified; access to Google Analytics restricted to relevant staff only. Analytics can only be accessed by relevant staff who have required level of access; account is password protected. We are soon to move from Universal Google Analytics to GA4 (July 2022), which will not store any IP addresses, thus reducing any privacy concerns further and this issue will become obsolete.	
22	Do you use pseudonymisation and/or anonymisation? If	FOR DATA TYPES at1 – 3: No. FOR DATA TYPE 4: AnonymizeIP feature is in use, ensuring the last three digits of website visitor's IP addresses are dropped as Google Analytics processes data.	

	so, give details.		
23	If you will use encryption, are you responsible for encrypting and decrypting the personal information that you process?	N/A	
24	Will you transfer, disclose or permit remote access to personal information to/from a country or territory outside of the EEA? If so, which ones?	No • We are about to adopt GA4 which drops the collection of IP addresses altogether, thus not transferring any data to US servers. Website hosting server is based in London, UK.	
25	Are measures in place to ensure an adequate level of security when the personal information is transferred outside of the EEA? What are they?	N/A	
26	Please explain the steps that will be taken to ensure "privacy by design and	A pre-DPIA was prepared before the project was approved to ensure privacy matters were considered from the outset and to determine whether a DPIA was required. This DPIA has been prepared whilst the project has developed and the Phase 1 website developed and built and will continue to be updated, revised and reviewed throughout the life	

	fault" as part of this project.	of the project and the Phase 1 website. Procurement to secure a contractor to develop, build and maintain the website included a range of data protection and privacy elements in the tender and selection process. Data Protection and UK GDPR requirements taken into account in contract Specification and contract provisions. We have adopted the approach of data minimisation, limiting all personal information collected or published on our website to the absolute minimum to conduct our function. As and when we've identified personal information through the life cycle of this project, we've assessed whether it was strictly necessary for the function of our website – this has resulted in minimal personal data being collected/stored etc. DPIA has been drafted and will be completed. Internal GDPR WP consulted on draft DPIA. DPO has considered and advised on draft DPIA. SMT to consider draft DPIA before approved and kept under review.	
27	What retention period(s) will be applied to the information?	FOR DATA TYPE 1 (Staff web admin details): As long as account active / staff member employed to carry out relevant duties; staff details from website administrator accounts will be removed on when staff leave or move to another post in the organisation which has different duties . FOR DATA TYPE 2 (Details of staff and events speakers on web pages): Varies - content reviewed per website maintenance programme and removed if out of date or no longer of value to website users. FOR DATA TYPE 3 (Commissioner's photo): Limited to the time Commissioner's remains in post. FOR DATA TYPE 4 (Website analytics): Information held by Google Analytics for 14 months – will be obsolete once moved to GA4 in July 2022.	*Consider any statutory requirements, legitimate business reasons or evidential reasons for retaining the information.* *Consider whether retention policy needs to be updated.*

Part B: Privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Additional columns may be required for additional risks in Parts B, C, D and E.

		Risk 1	Risk 2
28	Privacy risk	Potential for cyber attack on Phase 1 website leading to unauthorised access to personal data of types listed	Accidental or deliberate unauthorised processing or sharing of personal data used in the project and after the Phase 1 website launched
29	Risk to individuals	Risk to individuals/data subject of inappropriate and unauthorised use of personal data – risk of data incidents and data breaches	Risk to individuals of inappropriate and unauthorised use of personal data – risk of data incidents and data breaches
30	Compliance risk	Lack of compliance with 'UK GDPR principles and data protection requirements: Lawfulness, fairness and transparency; Purpose limitation; Data minimisation; Accuracy; Integrity and confidentiality (security); and Accountability.	Lack of compliance with principles of UK GDPR, including (depending on nature of accidental processing): Lawfulness, fairness and transparency; Purpose limitation; Data minimisation; Accuracy; Integrity and confidentiality (security); and Accountability.
31	Associated risks to the Commissioner	Reputational risk and financial risk relating to personal data incident or breach. Risk of enforcement action by ICO - enforcement notice or financial penalties and related reputational risk	Reputational risk and damage. Enforcement action by ICO – enforcement notice and financial penalties

Part C: Risk treatment

Describe the privacy treatment options or controls[1] that could be taken to reduce the risks identified above and any future steps that would be necessary (e.g., the production of new guidance or future security testing for systems).

		Risk 1				Risk 2		
		Risk Treatment 1	Risk Treatment 2	Risk Treatment 3	Risk Treatment 4	Risk Treatment 1	Risk Treatment 2	Risk Treatment 3
32	Potential treatment options and/or controls	[redacted] Exemptions 30(c), 35(1)(a), 39(1)				[redacted]		
33	Result: Is the risk eliminated, reduced, or accepted if the treatment(s)/control(s) is/are implemented?							
34	Evaluation: Is the final (i.e. residual) impact on individuals after implementing this treatment/control a justified, compliant and proportionate response to the aims of the project?							
35	Should this treatment/control be implemented? (If not,							

[1] Controls could include, for example, anonymisation, pseudonymisation, data minimisation, reducing the extent and purposes of processing, period of storage, accessibility or technical and organisational information security measures, such as those identified in ISO 27001.

	indicate the reason.)							
36	Decision taken by	HOCS	HOCS/HOPI	HOCS/HOPI	HOCS/HOPI	HOCS/HOPI	HOCS	HOCS/HOPI

Part D: Consultation feedback

To the extent that consultation has taken place with stakeholders/affected individuals/representatives, please summarise the feedback below.

		Risk 1	Risk 2
37	Feedback received	Assurances and evidence obtained from website contractor that all security measures relevant to our website have been implemented.	
38	Result: Is the risk eliminated, reduced, or accepted if the feedback is implemented?	Reduced – in current climate, difficult and inappropriate to consider that the risk eliminated.	
39	Evaluation: Is the final (i.e. residual) impact on individuals after implementing this feedback a justified, compliant and proportionate response to the aims of the project?	Yes - it is a justified, compliant and proportionate response	
40	Should this feedback be implemented? (If not, indicate the reason.)	Yes – all actions have been implemented.	
41	Decision taken by	HOCS/HOPI	
DPO consultation on draft DPIA and response			
HOCS consulted DPO on 08/06/22 Response from DPO received 21/06/22	I am happy with the content of the DPIA and do not have any comments or changes to the content. The DPIA is comprehensive in its terms and has been well prepared. Essentially, the risks to processing is low and for the most part the personal data involved is restricted to SMT in terms of business requirements and in the interests of transparency. I note that you have adopted a data minimisation approach to the website which is consistent with the purposes for the processing. Whilst Website Analytics will process IP addresses this will not result in the identification of individuals and, in any event, you are moving to GA4 which will not store IP addresses. For the personal data being processed privacy notices are in place and I'm assuming that this will also cover the entries in the Register of Interests for senior staff that are published on the website. Provision has been made for individual rights requests in terms of UK GDPR and the website (and DPIA) are to be kept under review. I would agree with the scoring for the assessment of likelihood and severity of risk as a 2.		

Part E: The DPIA outcomes and integration into the project plan

		Risk 1	Risk 2
42	Approved treatment(s)/control(s)	Exemptions 30(c), 35(1)(a), 39(1)	
43	Approved by	HOCS/ HOPI	
44	Action/next steps to be taken	Exemptions 30(c), 35(1)(a), 39(1)	
45	Date of completion of action	TBA	
46	Responsibility for action	HOPI/HOCS	

Part F: Overall risk assessment[2]

Note: use the table below to give an overall indication of your assessment of the risks posed by the project to personal information based on the answers given above. If the final overall risk assessment is that the residual risk of the processing is high, consult the ICO prior to processing.

	Severity of Risk					
Likelihood of Risk	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2 x	3	4	5	6
2	2	3	4	5	6	7
3	3	4	5	6	7	8
4	4	5	6	7	8	9
5	5	6	7	8	9	10

The overall risk assessment is 2

- the likelihood of risk is 1
- the severity of risk is 2

[2] To be completed by the Commissioner or the person responsible for data protection in the Commissioner's office.

Part G: DPIA declaration

I confirm that the data protection impact of this project to the relevant data subjects has been minimised to the extent reas onably possible to ensure that the processing of their personal information will not be unwarranted or unfairly prejudice their interests and that it is reasonable and proportionate to take the remaining risks in all the circumstances. I confirm that the use of the personal information described in this DPIA for the purposes of this project is necessary and justified and that the use of this personal information as part of this project should comply with all applicable data protection laws as at the date of this DPIA.

Person responsible for processing personal data	**Data Controller**
Exemptions 38(1)(b)	Signed
Name Helen Gardner-Swift	Name Daren Fitzhenry
Date 22/11/22	Date 23/11/22
Job title Head of Corporate Services	Job title Scottish Information Commissioner

Document control sheet

Document Information	
Full name of current version: Class, Title, Version No and Status. *E.g. C5 Key Documents Handbook v01 CURRENT ISSUE*	C5 DPIA Phase 1 New Website CURRENT ISSUE REDACTED VERSION
VC File Id	183850
Type	DPIA
Approver	SMT
Responsible Manager	HOPI
Date of next planned review	March 2024 or as required
Approval & Publication	
Approval Date (major version)	13/09/2022
For publication *(Y/N)*	Y
Date published	16/03/2023
Name of document in website file library	DPIA_Phase1_New_Website
Corrections / Unplanned or Ad hoc reviews (see Summary of changes below for details)	
Date of last update	

Summary of changes to document				
Date	**Action by** *(initials)*	**Version updated** *(e.g. v01.25-36)*	**New version number** *(e.g. v01.27, or 02.03)*	**Brief description** *(e.g. updated paras 1-8, updated HOPI to HOCS, reviewed whole section on PI test, whole document updated, corrected typos, reformatted to new branding)*
16/03/2023	LB	01.00	01.02	Redacted document created and DCS updated

Scottish Information Commissioner
Kinburn Castle
Doubledykes Road
St Andrews, Fife
KY16 9DS

t 01334 464610
f 01334 464611
enquiries@itspublicknowledge.info

www.itspublicknowledge.info