F4H
c/o RHQ RTR
Stanley Barracks,
Bovington, BH20 6JB

www.f4h.org.uk

1 Oct 2018

F4H General Data Protection Regulation (GDPR) – Data Protection Impact Assessment

References:

A. European General Data Protection Regulation (GDPR), 25 May 2018.
B. Information Commissioner's Office (ICO) GDPR: https://ico.org.uk/for-organisations/charity/
C. ICO Guide to GDPR: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
D. Reporting a Breach: https://ico.org.uk/for-organisations/report-a-breach/

Document Management Record

Originated: May 18

Next Full Document Review Date: Sep 19 (or as/if update required if earlier)

Document Status					
Issue	Date	Notes	Originator	Authorised by	Comments / Version
1	~~8 May 2018~~	~~Initial draft~~	~~CEO~~	~~CEO~~	~~Initial draft for comment~~
2	~~24 May 2018~~	~~Working Draft~~	~~CEO~~	~~CEO~~	~~Working Draft~~
3	Sep 2018	Final	CEO	CEO	V2
4					
5					
6					
7					
8					
9					

Contents

Data Protection Impact Assessment

Grading:

	Risk sufficiently mitigated
	Risk not mitigated in full but accepted
	Risk not mitigated in full but accepted with major caveats
	Risk not mitigated, not acceptable

Ser	Data protection issue	Reason	Assessment of risks	Mitigation measures[1]	Conclusion
	(a)	(b)	(c)	(d)	(e)
1.	**Purpose specification:** Is the data to be collected to be used only for a specified purpose? Will the data collected be used for anything other than the specified purpose?	Specified Purpose.	**Example**: "Function creep". **In practice:** Data shared (where required/appropriate) with mainstream military charities. Limited data shared with Brathay administration to enable delegates' comfort, personal support requirements and safety. Data collected at the beginning of each course for Brathay's governance, ensuring safety and comfort of delegates. Limited data to be shared with Brathay Research Hub (questionnaires, surveys, not 'Form A' details). Historical record keeping.	Delegates specifically told for what purpose data is collected. Legitimate Interest. Consent.	Risk sufficiently mitigated

[1] See also 'In Practice' of Assessment of Risk.

Ser	Data protection issue	Reason	Assessment of risks	Mitigation measures[1]	Conclusion
	(a)	(b)	(c)	(d)	(e)
			Brathay / military charities all have their own stringent data protection measures.		
2.	**Data limitation:** Is all the personal data collected necessary for the activity? When people engage with F4H seeking support, are they told how the personal information they supply will be used?	Processing adequate relevant and updated. Responsibility and accountability. Consent. Information and access.	**Example**: Some organisations may collect more personal data than necessary for the specified purpose. **In practice**: Organisations can suffer reputational damage when it becomes publicly known that staff are collecting more personal data than they actually need. The additional personal data collected creates a bigger risk for the delegates, their families or others if the system is hacked or otherwise compromised (unauthorized use/disclosure or security breach). Collecting more detail than needed also increases the risk of identity fraud or theft. F4H does not collect more data than is absolutely necessary to undertake its function.	Ensure data collected are only those which are necessary to achieve the purpose specified. Give delegates prior notice regarding the purposes of the data collection and processing. Give delegates an opportunity to question the manner and purpose for which their data is collected and processed.	Risk sufficiently mitigated
3.	**Right to information:** Are individuals explicitly informed about why their	Information and access	**Example**: Organisations do not provide individuals with clear and easily accessible information regarding their	Delegates specifically told where and for what purpose data is collected. Legitimate Interest.	Risk sufficiently mitigated

Ser	Data protection issue	Reason	Assessment of risks	Mitigation measures[1]	Conclusion
	(a)	(b)	(c)	(d)	(e)
	personal data is being collected and how it may be used?		policies, procedures and practices on the collection of information. If data collection/processing standards and procedure are not transparent, individuals may not trust the charity and refrain from providing their personal data. **In practice**: All data collection and use by all F4H volunteers must be transparent, honest, the minimum required.	Consent. Published to F4H website includes this DPIA, the charity's GDPR Data Protection Policy and Privacy Notice. All F4H volunteers will explain to the data subject initially and on follow-up (if required) all data processing requirements.	
4.	**Legal basis for data processing/transfer:** **Consent** Are individuals able to appreciate the most likely consequences (including negative)? Does the person have a genuine free choice as to whether to consent? How do individuals provide consent for their information to be collected? Has the delegate explicitly agreed to how their information can be used, or that it can be shared with other agencies?	Purpose specification. Lawful and fair processing. Consent. Information and access.	**Example**: One or more individuals threaten to announce publicly that they did not give their consent to the collection of their personal data. If consent is not written, are any risks involved? Damage to the charity's reputation if not adhered to. Is consent limited to a specified purpose? **In practice**: F4H does not routinely obtain a signed form from the individual consenting to the collection and use of his or her personal data.	It is explained to potential delegates and/or other relevant parties the implications of providing their data to F4H. It is explained how their data could be used and to whom it could be further transferred. If possible, a signed informed consent form is obtained. However, this is not a routinely workable solution. Consent, when given verbally is recorded. **A record of the time, date and how ('phone call, face-to-face, text) is made at the time of the conversation including what was said/agreed.** **Outreach/Administration ensure this the record is maintained and is accurate.**	Risk sufficiently mitigated

Ser	Data protection issue	Reason	Assessment of risks	Mitigation measures[1]	Conclusion
	(a)	(b)	(c)	(d)	(e)
	Are there instances or circumstances where a delegate has consented to the sharing or disclosure of personal information, but where the staff does not think it is wise to do so?		Consent is first agreed and recorded.	The consent record is consistent and accessible across all methods of collection.	
5.	**Alternative legal Basis:**	Governance	If after consent given, delegate attended a course, there can be the process/transfer of additional personal data questionnaires/surveys) on an alternative legal basis (vital interest, public interest, **legitimate interest**, compliance with a legal obligation).	If informed consent is not obtained it will usually mean the delegate cannot proceed further or attend a course.	Risk sufficiently mitigated
6.	**Right to access / Rectification / Deletion:** Are individuals provided with the possibility to access and correct their personal information? Can they request the deletion of some or all of their personal information? Is it necessary to restrict access to data? If so, are these restrictions adequately circumscribed and explained?	Information and access. Rectification and deletion.	**Example**: Some individuals may wish to see and, if necessary, amend (or have deleted) their personal data. Reputation damage possible if individuals' complaints are not addressed. **In practice**: Delegates may request to see their data held by F4H and opt to have it amended or deleted.	F4H has specific/transparent procedures to provide data subjects access to their personal data. F4H DP Policy stipulates that data subjects can gain access to their data IAW EU GDPR 2018. F4H's DP Policy, Privacy Notice and this DPIA are published to the charity's website.	Risk sufficiently mitigated

Ser	Data protection issue	Reason	Assessment of risks	Mitigation measures[1]	Conclusion
	(a)	(b)	(c)	(d)	(e)
7.	**Information quality and accuracy:** Is the data relevant, reliable and accurate? Is there a policy or procedure in place to correct data that has already been shared with partners, or to notify partners about updates?	Processing adequate, relevant and updated data. Rectification and deletion. Objection	**In practice**: F4H volunteers do not have enough time and sufficient resources to check the reliability of all the information they receive from the delegates. F4H staff may have to rely on incomplete information or information they are unable to verify – this may include information provided by referral from a third party. F4H staff may take decisions based on incomplete, unreliable or false information. Poor quality information might lead to inappropriate decisions.	Where possible, information is cross-check from an individual with other organizations who may also have interviewed the individual or other witnesses[2]. Proof of service, proof of financial situation is sometimes needed, or is collected by representatives of third-party benevolent charities collecting information on behalf of F4H. Information is taken in good faith, checked where possible (this may include a 'gut instinct' linked to experience that the delegate is legitimate serving or former service personnel). Where necessary, third party with whom data has been shared will be informed of updates/an individual's wish 'to be forgotten'.	Risk not mitigated in full but accepted
8.	**Appropriate security measures:** What personal information is collected? Could disclosure of this information put the person in danger (for example information relating to ethnicity, religion, sexual	Security. Data breaches. Responsibility and accountability.	**Example**: External hackers and rogue volunteers may seek to exploit personal data. **In practice**: F4H imparts to volunteers good information security practices, reinforced by direction given in F4H	Encourage (warn) employees to limit use of unsecured portable storage devices, such as memory sticks. Develop robust access control protocols which limit access on a 'need to know' basis. Users should only have access to that portion of data they need to carry out their legitimate functions.	Risk not mitigated in full but accepted

[2] GDPR states that the referring third-party organisation will have obtained the data subject's permission to refer and pass their data.

Ser	Data protection issue	Reason	Assessment of risks	Mitigation measures[1]	Conclusion
	(a)	(b)	(c)	(d)	(e)
	orientation, political views, trade union membership, etc.) Is there a risk of information being stolen / lost / altered / rendered unavailable / system hacked / organisation subject to surveillance? What preventative measures are in place? Does the processing involve external organisations or third parties? Does this increase the risk of surveillance / disclosure by the processor (whether lawfully or not) / hacking / data theft / availability? Is information limited to others on a "need to know" basis? How is this implemented in practice? Are staff reminded to keep paper files, CDs and/or memory sticks locked up or with them at all times when they are not in use?		GDPR DP Policy Document and training and briefings. Volunteers are instructed to use strong passwords across all IT. All volunteers working with F4H have a background of strong information security (military, The Brathay Trust, national universities working with student data). Third-party organisations with whom data may be shared (main-stream service benevolent charities) have their own stringent measures in place. F4H emails are encrypted[3]. Any data breach will be acted upon within the requirements of the EU GDPR 2018, as highlighted in F4H's DP Policy Document.	Ensure clarity re who has the authority to assign, change or revoke access privileges. Ensure all accesses to the databases are logged into a register of processing operations. Set-up data breach notification procedures to inform the data subjects.	

[3] The charity's email is hosted within a secure datacentre on a managed platform which is monitored and regularly updated. All communication with the email server is encrypted, protecting both user credentials and email content in transit. (Integrous Ltd, Mar 18). Our website is hosted within a secure datacentre on a managed platform which is regularly updated. All communications with the website are encrypted using an SSL certificate and the website software itself is maintained and regularly updated.

Ser	Data protection issue	Reason	Assessment of risks	Mitigation measures[1]	Conclusion
	(a)	(b)	(c)	(d)	(e)
	Is training given to all staff on good data protection and information security practices? Are e-mails encrypted? What action will be taken if there is a data breach?				
9.	**Data sharing, disclosure/publication and/or transfer:** Will the personal information be shared with or disclosed to other organisation? Why? Does the organisation have an adequate data protection policy? Has the individual data subject explicitly agreed to the sharing of their data?	Transfers Accountability and Responsibility Confidentiality Processing Adequate Relevant and Updated Data Data Security Publication	**Example**: Volunteers may share personal data with other organizations or authorities over which they have no control regarding how the other organizations or authorities may use that data or further share it. Publications of photographs could attract attention from unwarranted individuals. The data subject can be put at risk if the organisation does not process the data according to adequate data protection standards. Individuals may complain about the disclosure of their data **In practice**: F4H shares data only with recognised, bone fide organisations Where promotional videos, brochures or press stories are developed, F4H	Personal information is shared with other organizations only if a specific legal basis exists. F4H shares personal information with other organizations or authorities only if there is a specific need to do so (see above regarding third-party charitable organisations) and they observe appropriate data protection measures Stringent consent records are maintained if information is to be shared with third-party organisations (eg: Form As, The ABF for promotional information; The Brathay Trust promotional videos).	Risk sufficiently mitigated

Ser	Data protection issue	Reason	Assessment of risks	Mitigation measures[1]	Conclusion
	(a)	(b)	(c)	(d)	(e)
			acquires consent or personal information is anonymised.		
10.	**Data retention:** Is personal information being entered into databases? Is it necessary to keep all of the data that is being processed? Are there procedures for reviewing how long data should be retained? Is there a policy, procedure, rationale for archiving personal information? Is too much data being kept for auditing purposes? Could this be minimised?	Data Retention	**Examples**: The personal data originally collected is collected without specifying the retention period and is kept for an unlimited period Data recorded are not necessary anymore to fulfil the purpose for which they were originally collected **In practice**: Personal data is collected and routinely retained for a maximum of 5 years[4]. F4H may keep data for longer if it cannot be deleted for legal, regulatory or technical reasons. F4H may also keep it for research or statistical purposes. If so, F4H will make sure that privacy is protected and only used it for those purposes.	The retention of personal data is limited to what is necessary to fulfil specific, explicit and legitimate purposes. The data retention period is specified in our Privacy Notice.	Risk sufficiently mitigated
11.	**Accountability/Oversight mechanism:** Are data protection standards and procedures effectively implemented?	Good Governance	**Example**: There are no documented and communicated data protection policies, procedures and practices. No accountability has been assigned to anyone for data protection.	**Example**: A data protection focal point is entrusted with the specific responsibility for ensuring the adequacy of F4H's policies, procedures and practices.	Risk sufficiently mitigated

[4]An initial retention period could be extended if it is considered necessary to keep the data to fulfil the purpose for which it was originally collected.

Ser	Data protection issue	Reason	Assessment of risks	Mitigation measures[1]	Conclusion
	(a)	(b)	(c)	(d)	(e)
	Are oversight mechanisms in place to overview existing practices and to provide guidance?		No one has been assigned responsibility for the transfer of personal data to a third party and that the third party with whom it shares personal data comply with data protection standards to the same degree has not been verified **In practice**: F4H documentation distributed to all volunteers and supporters as well as published to our website include: EU GDPR 2018 DP Policy, Data Protection Impact Assessment and our Privacy Notice. Volunteers are reminded of DP responsibilities on a regular basis through Newsletters, Symposiums and trg opportunities.	Although no DPO is nominated (F4H is not a public-sector organisation nor undertakes '…*regular and systematic monitoring* [of data subjects] *on a large scale*' either special category or otherwise), the CEO is responsible for overseeing and setting practices. Charity volunteers are encouraged to watch/learn form ICO-sanctioned training videos and information, as well as receiving ICO-produced posters	