Data Privacy Impact Assessment

Introduction

Convert Insights customers have an expectation that their privacy and confidentiality will be respected at all times. It is essential therefore, when considering or implementing any changes, that the impact of the collection, use and disclosure of any personal information is considered in regards to the individual's privacy. Carrying out a privacy impact assessment (PIA) is a systematic way of doing this.

A PIA will help Convert Insights to identify privacy risks and ensure lawful practice when a new project is designed or changes are made to a service. The purpose of the PIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible.

What are privacy risks?

Privacy risks include the following:

- Risks to individuals or other third parties (for example, misuse or overuse of their personal data, loss of anonymity, intrusion into private life through monitoring activities, lack of transparency).
- Compliance risks e.g. breach of the General Data Protection Regulation (GDPR)
- Risks to the organisation (for example, failure of the project and associated costs, legal penalties or claims, damage to reputation, loss of trust of customers or the public).

Where do we start?

A lead person was nominated to coordinate the PIA process (dionysia@convert.com).

A PIA starts with a screening process. The screening questions are provided in the table on the next page. Answering the screening questions identified whether or not customer's privacy is impacted and whether or not we needed to complete a full PIA.

PIA screening questions

Documenting here which of the screening questions are applicable will help to draw out the particular privacy considerations that will help formulate your risk register later in the template. This will also assist in ensuring that the investment the organisation makes is proportionate to the risks involved:

		Yes	No	Unsure	Comments
i	Is the information about individuals likely to raise privacy concerns or expectations?	☐	☒	☐	**No personal data is used or stored in Convert Experiences.** Notes for transparency: **On by default** • Currently session cookie ID (timeout 20 minutes on cookie and server cache). Currently falling under performance cookies in our interpretation of GDPR / ePrivacy Directive and upcoming ePrivacy Regulations. **Off by default** • When cross browser targeting is turned on by the customers we insert unique cookie in URL to pick-up on the other domain (could be interpreted by GDPR as personal data). This feature is off by default

					as part of our privacy by default policy. • When a unique visitor IDs are given by the customer to replace session IDs this could be interpreted as personal data This feature is off by default as part of our privacy by default policy. • When geotargeting is used (not on my default) we could store country, region and city in CDN or server cache for correct targeting.
ii	Will Convert Insights involve the collection of new information about individuals?	☐	☒	☐	No, there is not such a plan defined and if there is a need for this, a PIA will be re-conducted and it will be communicated well in advance.
iii	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	☐	☒	☐	No. These are the places where we collect information: • Information We Collect When You Register and Create An Account • Information We Collect When You Register for a Webinar • Information We Collect When You Register for receiving the Newsletter • Information We Collect From Your Websites

					• Cookies And are described in detail in our Privacy Policy.
iv	Will you contact individuals in ways which they may find intrusive?	☐	☒	☐	No, we updated all our forms (free trial, lead magnet pages, newsletter, webinars) and we specifically mention in which ways data subjects will be contacted either through new checkboxes or with clear Privacy Notices..
v	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	☐	☒	☐	No, access is only restricted to Convert Insights members as defined in our IT Security Policy. In addition, Convert's Data Management Policy defines three roles for accessing data: • Data Controller who has the responsibility to ensure that appropriate data management policies are in place so that the data owners can ensure they are compliant with legislation to the best of their ability. • Data Owner who authorise the access and use of data, regularly review access privileges, assess the risks, ensure that appropriate contingency plans

					are in place to safeguard the data. • Data Custodian to whom in some cases data will be entrusted (e.g. an individual or a third party company) for the purposes of storage and/or processing.
vi	Will the information be likely to result in a high risk to the rights and freedoms of natural persons? (See Article 29 Working Party)	☐	☒	☐	No, the information Convert Insights collects will not result in a high risk as defined in GDPR and listed below: • Discrimination • Identity theft / fraud, financial loss • Reputation damage • Loss of confidentiality of personal data protected by professional secrecy • Unauthorised reversal of pseudonymisation • Any other significant economic or social disadvantage • Individuals deprived of rights and freedoms, or prevented from exercising control over their data • Processing sensitive data,

including data on racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership; genetic data; health data; data concerning sex life; or data on criminal convictions and offences or related security measures
- Profiling (personal aspects are evaluated [e.g. analyse or predict work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements] to create or use personal profiles)
- Processing children's and vulnerable persons' data
- Processing large amounts of data affecting large numbers of individuals

vii	Will you make decisions or take action against individuals in ways which can have a significant impact on them?	☐	☒	☐	No, Convert Insights does not make any decisions or take action against individuals with significant impact on them.
viii	Will you use new technology which might be perceived as being privacy intrusive?	☐	☒	☐	No, Convert Insights does not use such technologies e.g. biometrics, facial recognition, or profiling.

If you answered "**No**" to all of the above, and you can evidence/justify your answers in the comments box above, you do not need to continue with the Privacy Impact Assessment as it will not apply.

If you answered "**Yes**" or "**Unsure**" to any of the screening questions in the table, you will need to undertake the PIA.

Conducting a PIA

What should a PIA include?

In simple terms the PIA should:

- explain why the PIA is necessary (the initial screening questions at the beginning of the template will enable this to be quickly identified)
- document the data flows in terms of, what data is being processed, where it is coming from and who it is going to
- identify the risks to individual's privacy in terms of security, and as potential threats to confidentiality, integrity or availability
- clarify the legal basis
- Identify and evaluate the privacy solutions (how can you reduce or remove the risk?)
- Sign off and record the PIA outcomes
- Integrate the outcomes into the project plan
- Consult with internal and external stakeholders, as needed, throughout the process

Who should be part of the PIA team needed to complete the template?

For the PIA to be effective it needs input from people with a range of expertise, skills and authority. Important features for members of the team include:

- An understanding of the project's aims and the organisation's culture;
- Authority to influence the design and development of the project and participate in decisions;
- Expertise in privacy and compliance matters;
- Ability to assess and communicate organisational risks;
- Ability to assess which privacy solutions are feasible for the relevant project; and
- Ability to communicate effectively with stakeholders and management.

Does my project need a PIA?

If your project is new, or you are planning changes to an existing system, then the time is right for conducting a PIA. A PIA is suitable for:

- A new IT system for storing and accessing personal data
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data
- A proposal to identify people in a particular group or demographic and initiate a course of action
- Using existing data for a new and unexpected or more intrusive purpose
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system
- A new database which consolidates information held by separate parts of an organisation
- Legislation, policy or strategies which will impact on privacy through the collection of personal information, or through surveillance or other monitoring
- Long standing databases where the privacy impact may not have been considered previously or the legal or organisational framework has changed and may give rise to new privacy risks or issues

Privacy Impact Assessment Template

Section 1: Background Information

Project Name	
Organisation	
Assessment Completed By	
Job Title	
Date completed	
E-mail	
Date reviewed	

Project/Change Outline - What is it that is being planned? A brief description of the project/process being assessed is required.

Purpose / Objectives - Why is it being undertaken? This could be the objective of the process or the purpose of the system being implemented as part of the project.

What is the purpose of collecting the information within the system?

What are the potential privacy impacts of this proposal - how will this change impact upon the data subject? Provide a brief summary of what you feel these could be, it could be that specific information is being held that hasn't previously or that the level of information about an individual is increasing.

Provide details of any previous Privacy Impact Assessment or other form of personal data compliance assessment done. If this is a change to an existing system, a PIA may have been undertaken during the project implementation

Stakeholders - who is involved in this project/change? Please list stakeholders, including internal, external, organisations (public/private/third) and groups that may be affected by this system/change.

Section 2: The Data Involved

What data is being collected, shared or used?
(If there is a chart or diagram to explain attach it as an appendix)

Data Type	**Justifications –** there must be justification for collecting the particular items and these must be specified here – consider which data items you could remove, without compromising the needs of the project?

Information that identifies the individual and their personal characteristics	Name	☐
	Address	☐
	Postcode	☐
	Job	☐
	Age	☐
	Sex	☐
	Gender	☐
	Racial/ethnic origin	☐
	Tel no.	☐
	Mobile/home phone no.	☐
	Email address	☐

	Yes	N/A	**Justification**
Information relating to the individual's physical or mental health or condition	☐	☐	
Information relating to the individual's sexual life	☐	☐	
Information relating to the family of the individual and the individuals lifestyle and social circumstances	☐	☐	

Information relating to any offences committed or alleged to be committed by the individual	☐	☐
Information relating to criminal proceedings, outcomes and sentences regarding the individual	☐	☐
Information which relates to the education and any professional training of the individual	☐	☐
Employment and career history	☐	☐
Information relating to the financial affairs of the individual	☐	☐
Information relating to the individual's religion or other beliefs	☐	☐
Information relating to the individual's membership of a trade union	☐	☐

Section 3: Assessment

	Question	Response	Required Action **E.g. Seek Information Governance advice**

Legal compliance – is it fair and lawful?	1. What is the legal basis for processing the information? *This should include which conditions for processing under the GDPR apply and the common law duty of confidentiality.*		
	2.a Is the processing of individual's information likely to interfere with the data subject rights as defined under GDPR? 2.b Have you identified the social need and aims of the project and are the planned actions a proportionate response to the social need?		
	3. It is important that individuals affected by the initiative are informed as to what is happening with their information. Is this covered by fair processing information already provided to individuals or is a new or revised communication needed?		

	4. If you are relying on consent to process personal data, how will consent be obtained and recorded, what information will be provided to support the consent process and what will you do if permission is withheld or given but later withdrawn?		
Purpose	5. Does the project involve the use of existing personal data for new purposes?		
	6. Are potential new purposes likely to be identified as the scope of the project expands?		
Adequacy	7. Is the information you are using likely to be of good enough quality for the purposes it is used for?		
Accurate and up to date	8. Are you able to amend information when necessary to ensure it is up to date?		
	9. How are you ensuring that personal data obtained from individuals or other organisations is accurate?		
Retention	10. What are the retention periods for the personal information and how will this be implemented?		

	11. Are there any exceptional circumstances for retaining certain data for longer than the normal period?		
	12. How will information be fully anonymised or destroyed after it is no longer necessary?		
Rights of the individual	13. How will you action requests from individuals (or someone acting on their behalf) for access to their personal information once held?		
Appropriate technical and organisational measures	14. What procedures are in place to ensure that all staff with access to the information have adequate information governance training?		
	15. If you are using an electronic system to process the information, what security measures are in place?		
	16. How will the information be provided, collated and used?		
	17. What security measures will be used to transfer the identifiable information?		

Transfers both internal and external including outside of the EEA	18. Will individual's personal information be disclosed internally/externally in identifiable form and if so to who, how and why?		
	19. Will personal data be transferred to a country outside of the European Economic Area? If yes, what arrangements will be in place to safeguard the personal data?		
Consultation	20. Who should you consult to identify the privacy risks and how will you do this? Identify both internal and external stakeholders.		
	21. Following the consultation – what privacy risks have been raised? E.g. Legal basis for collecting and using the information, security of the information in transit etc.		
Guidance used	22. List any national guidance applicable to the initiative that is referred to.		

Section 4: Privacy issues identified and risk analysis

a) Identify the privacy and related risks (see Appendix 1 for further information)

Nb. By allocating a reference number to each identified privacy issue will ensure you link back to this throughout the rest of the assessment. Column (a), (b) and/or (c) must be completed for each privacy issue identified in column

Table 1

Ref No.	**Privacy issue –** element of the initiative that gives rise to the risk	**(a) Risk to individuals** *(complete if appropriate to issue or put not applicable)*	**(b) Compliance risk** *(complete if appropriate to issue or put not applicable)*	**(c) Associated organisation/corporate risk** *(complete if appropriate to issue or put not applicable)*
Example PR1	*Individuals are not aware of the project as no communication materials have been planned*	*Individuals not aware that their data is being processed*	*Non-compliance with GDPR – fair and lawful processing*	1. *May lead to public mistrust*

b) Identify the privacy solutions

Table 2

Ref No.	**Risk – taken from column (a), (b) and/or (c) in table 1.**	**Risk score – see tables at Appendix 2**			**Proposed solution(s) /mitigating action(s)**	**Result:** is the risk accepted, eliminated, or reduced?	**Risk to individuals is now OK? Signed off by?**
		Likelihood	**Impact**	**RAG status**			

Example PR1	*Individuals not aware that their data is being processed* *Non-compliance with GDPR – fair and lawful processing* *1. May lead to public mistrust*	5	5		*Communication plan to be developed to ensure compliance with fair and lawful processing* *Assurance that there will be an active communication campaign* *All relevant staff informed of need to understand and disseminate communication material.*	*Reduced to an acceptable level (it is not possible to eliminate at this stage as the Comms plan will need to ensure it addresses all aspects to enable individuals to be fully informed.*	*Yes* *Sign-of tbc*

c) Integrate the PIA outcomes back into the project plan

NB. This must include any actions identified in Table 1 and Table 2.

Who is responsible for integrating the PIA outcomes back in to the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?							
Ref No.	**Action to be taken**	**Date for completion of actions**	**Anticipated risk score following mitigation**			**Responsibility for action – *job title not names***	**Current status/progress**
			Likelihood	**Impact**	**RAG status**		
Example PR1	*Communications plan to be developed*		*2*	*2*		*Project Manager to liaise with Communication lead and embed into project plan*	*Meeting arranged with Communication Lead*

Appendix 1: Types of privacy risk

Risks to individuals

- Inappropriate disclosure of personal data internally within your organisation due to a lack of appropriate controls being in place.
- Accidental loss of electronic equipment by organisation's personnel may lead to risk of disclosure of personal information to third parties.
- Breach of data held electronically by "hackers".
- Vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate disclosure of personal data.
- Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen turn out not to be effective.
- Personal data being used in a manner not anticipated by data subjects due to an evolution in the nature of the project.
- Personal data being used for purposes not expected by data subjects due to failure to explain effectively how their data would be used.
- Personal data being used for automated decision making may be seen as excessively intrusive.
- Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals.
- Merging of datasets may inadvertently allow individuals to be identified from anonymised data.
- Use of technology capable of making visual or audio recordings may be unacceptably intrusive.
- Collection of data containing identifiers may prevent users from using a service anonymously.
- Data may be kept longer than required in the absence of appropriate policies.
- Data unnecessary for the project may be collected if appropriate policies not in place, leading to unnecessary risks.
- Data may be transferred to countries with inadequate data protection regimes.

Compliance risk

- Non-compliance with the common law duty of confidentiality
- Non-compliance with the GDPR.
- Non-compliance with sector specific legislation or standards.
- Failure to carry out a DPIA where appropriate is itself a breach of the legislation, as well as a lost opportunity to identify and mitigate against the future compliance risks a new project may bring.

Corporate risks

- Failure to comply with the GDPR may result in investigation, administrative fines, prosecution, or other sanctions. Failure to adequately conduct a DPIA where appropriate can itself be a breach of the GDPR.
- Data breaches or failure to live up to customer expectations regarding privacy and personal data are likely to cause reputational risk.
- Public distrust of your organisation's use of personal information may lead to a reluctance on the part of individuals to deal with your organisation.
- Problems with project design identified late in the design process, or after completion, may be expensive and cumbersome to fix.
- Failure to manage how your company keeps and uses information can lead to inefficient duplication, or the expensive collection and storage of unnecessary information. Unnecessary processing and retention of information can also leave you at risk of non-compliance with the GDPR.
- Any harm caused to individuals by reason of mishandling of personal data may lead to claims for compensation against your organisation. Under the GDPR you may also be liable for non-material damage.

Appendix 2: Guidance for completing a risk register

- What is the actual risk? Make sure the risk is clear and concise and articulated with appropriate use of language, suitable for the public domain.
- Be careful and sensitive about the wording of the risk

- Don't reference blame to other organisations in the risk register (the register may be made available in the public domain)
- Does the risk belong to a business area within your organisation or another body?

It is common to use a RAG matrix rating system for assessing risk. RAG stands for red, amber, green. To achieve a RAG rating, each risk first needs a likelihood and impact score. Each risk will be RAG rated by taking the likelihood and impact scores, and using the matrix below:

Likelihood

	Score				
Likelihood score	1	2	3	4	5
Descriptor	Rare	Unlikely	Possible	Likely	Almost Certain
Frequency - how often might it happen?	This probablywill never happen/recur	Do not expect it to happen/recur, but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur, but is not a persisting issue or circumstance	Almost certain to happen/recur; possibly frequently

Impact

	Score				
Impact score	1	2	3	4	5
Descriptor	Very low	Low	Medium	High	Very high
Impact should it happen?	Unlikely to have any impact	May have an impact	Likely to have an impact	Highly probable it will have a significant impact	Will have a major impact

Using the risk "RAG" rating system for scoring risks means risks can be ranked so that the most severe are addressed first. Decisions can then be made as to what mitigating action can be taken to alleviate the risk.

Impact						
	Very High -5	A	A/R	R	R	R
	High - 4	A	A	A/R	R	R
	Medium - 3	A/G	A	A	A/R	A/R
	Low - 2	G	A/G	A/G	A	A
	Very Low - 1	G	G	G	G	G
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
		Likelihood				