

# Data Protection - Privacy Impact Assessment<sup>1</sup>

## Introduction

Individuals have an expectation that their privacy and confidentiality will be respected at all times. It is essential therefore, when considering or implementing any new initiatives, 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 Data Protection Impact Assessment (DPIA) is a systematic way of doing this.

In addition, the UK General Data Protection Regulation make it mandatory for DPIAs to be carried out where processing is likely to result in a high risk to the rights and freedoms of individuals and specifies a need to report this to the Information Commissioners Office prior to processing this information, where these high risks cannot be appropriately mitigated.

A DPIA helps an organisation to identify privacy risks and ensure lawful practice when a new project or system is designed or changes are made to a service. The purpose of the DPIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. It is a particularly useful tool for organisations to identify privacy risks and ensure lawful practice use when:

- Planning a new information sharing initiative such as working with new partners or in different ways;
- Introducing new IT systems for collecting and accessing personal data;
- Intending to use personal data for new uses.

## 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 Data Protection Act or the General Data Protection Regulation
- Risks to the organisation (for example, failure of the project and associated costs, legal penalties or claims, damage to reputation, loss of trust of service users, clients or the public).

## Where do you start?

A lead person should be nominated to co-ordinate the DPIA process.

---

<sup>1</sup> This DPIA template has been developed from an original PIA template created by the Information Governance Alliance and has been adapted for more general use and to meet the requirements of the General Data Protection Regulation

A DPIA starts with a screening process. The screening questions are provided in the table on the next page. Answering the screening questions will identify whether or not the proposed initiative will impact on privacy and whether or not you need to complete a full DPIA. The screening questions are designed to give you a quick sense of the scale of the privacy issues that you may be facing.

If you answer “yes” or “unsure” to any of the screening questions in the table, you will need to undertake the full DPIA. You may find it helpful to seek assistance from an information governance expert to help you with the process.

## DPIA Screening Questions

Documenting here which of the screening questions are applicable to your initiative 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	Does initiative involve the processing of Personal data?	<input checked="" type="checkbox"/>			Personal information will be both collected and processed as part of the new We collect Tyres website sales platform.
ii	Is the information about individuals likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The data collected through the website, the online sales process and the collection of personal information such as email addresses in order to create a mailing list is generally considered to be usual practices sales cannot be completed through the site, it is just basic contact information
iii	Will the initiative involve the collection of new information about individuals?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	New information will be collected through the website which is an extension of our usual business.
iv	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Although our current processes include the sale of products to companies and sole traders, this website allows potential customers to give us permission for regular marketing to be sent to them.

v	Will the initiative require you to contact individuals in ways which they may find intrusive <sup>2</sup> ?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>As part of the online sales process users will be contacted (primarily via email), to confirm their order, or to provide updates regarding their order.</p> <p>In order to promote the business, an online mailing list will be created. HELM will rely on “soft opt in” for marketing communications for similar services only. Users of the website will be able to ‘opt out’ when they make an enquiry for tyre disposal. Some individuals may find this intrusive, but will have the option to stop such communications (by unsubscribing).</p> <p>This will only be for business customers, the service is not expected to be used by individuals.</p>
vi	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p>User’s personal information will be disclosed to third party service providers which is necessary for the website to operate.</p> <p>The third party providers include:</p> <ul style="list-style-type: none"> <li>• Mayfly - web design and hosting company.</li> <li>• Mail Chimp - Mailing list provider.</li> </ul>
vii	Does the initiative involve you using new technology which might be perceived as being privacy intrusive e.g. biometrics or facial recognition?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>No, there is nothing biometric, the only details being gathered are name, contact number and email add.</p>
viii	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>No, there will be no decisions made about action against individuals</p>

<sup>2</sup> Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages

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 DPIA as it will not apply to the initiative. Should the initiative change to incorporate informational privacy at any point in the future you will need to complete the screening questions again.

# Privacy Impact Assessment Template

## Section 1: Background Information

Project Name	We Collect Tyres
Organisation	Hargreaves (UK) Services Limited (t/a We Collect Tyres)
Assessment Completed By	Arron Butta
Job Title	Head of Commercial
Date completed	January 2024
Phone	
E-mail	Arron.butta@hsgplc.co.uk

**Project/Change Outline - What is it that is being planned? If you have already produced this as part of the project's Project Initiation Document or Business Case etc. you may make reference to this, however a brief description of the project/process being assessed is still required.**

**We are planning to offer our service on tyre disposal through our website and offer a contact opportunity to businesses that are looking for our service.**

**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.**

**In order to increase sales volumes and generate profit margins.**

**What is the purpose of collecting the information within the system? For example patient treatment, patient administration, research, audit, reporting, staff administration etc.**

**To be able to facilitate:**

- An online sales contact platform
- Illustrate our service to prospective customers
- A customer database for marketing purposes

**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.**

Potential customers will be sending their contact information which may then be used as part of regular marketing campaigns.

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

No previous DPIA has been completed in relation to this project

**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.**

Stephen Barker - Managing Director

John Watson - Finance Director

Matthew Wilkinson- General Manager

Arron Butta- Head of Commercial

James Niven - Business Development Executive

David Hankin - Solicitor and Data Protection Officer

Mayfly - web design and hosting company.

Mail Chimp - Mailing list provider.

---

## 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 - Personal Data			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	<input checked="" type="checkbox"/>	This information allows us to contact the prospective customer about their enquiry and keep them up to date with our service in future.
	Address	<input type="checkbox"/>	
	Postcode	<input type="checkbox"/>	
	Dob	<input type="checkbox"/>	
	Age	<input type="checkbox"/>	
	Sex	<input type="checkbox"/>	
	Gender	<input type="checkbox"/>	
	Tel no.	<input checked="" type="checkbox"/>	
	Physical description	<input type="checkbox"/>	
	Identifier - NHS no./NI No, etc.	<input type="checkbox"/>	
	Mobile/home phone no.	<input type="checkbox"/>	
	Email address	<input checked="" type="checkbox"/>	

Data Type - Special Categories Data	Yes	N/A	Justification
Racial/Ethnic Origin	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Physical or mental health	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Sexual orientation/sexual life	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Criminal convictions and offences	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Religious or philosophical beliefs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

---

Trade Union membership

Political opinions

Identifiable genetic or biometric data

Any other data identifiable to an individual not specified above (please detail)

---

### Section 3: Assessment

	Question	Response	Required Action
<b>Data Protection Principles</b>			
Principle 1 - is it fair and lawful?	1. What is the legal basis for processing the information (considering both personal data and sensitive/special categories data)? <i>This should include which conditions for processing under the General Data Protection Regulation apply, and the common law duty of confidentiality.</i>	The legal basis for processing is consent for the initial enquiry (and soft opt in for future marketing emails).	HELM to ensure: (a) that the website enquiry form includes an option to opt out of marketing communications; (b) marketing is restricted to similar services to comply with the principles of soft opt in.
	2. a - Is the processing of individual's information likely to interfere with the 'right to privacy' under Article 8 of the Human Rights Act?  b - Have you identified the social need and aims of the initiative and are the planned actions a proportionate response to the social need?	a/No  b/ No issues identified.	No further actions identified.
	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?	The website will display a pop-up message with link to the privacy policy. The enquiry form will also include a link to the privacy policy.	Specified in website build to clearly provide the relevant information to the users of the website.
	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?	As above, when visiting the website a clear box will be displayed for the user to read and accept the privacy policy.	No further actions identified.
Principle 2 - Specified and legitimate	5. Does the project involve the use of existing personal data for new purposes?	NO	

	6. Are potential new purposes likely to be identified as the scope of the project expands	No	N/A
Principle 3 - Adequate, relevant and not excessive	7. Is the information you are using likely to be of good enough quality for the purposes it is used for?	Yes	N/A
Principle 4 - Accurate and up to date	8. Are you able to amend information when necessary to ensure it is up to date?	Yes	N/A
	9. How are you ensuring that personal data obtained from individuals or other organisations is accurate?	The user will be inputting their own information into the site through an enquiry form.	No further actions identified
Principle 5 - Retention (kept no longer than necessary)	10. What are the retention periods for the personal information and how will this be implemented?	Information will be kept for as long as individual does not opt out of communications. Where an individual opts out of communications, the customer will be deleted from the customer database save that data related to any contracts with the customer will be retained in accordance with the Document Retention Policy on Sharepoint.	
	11. Are there any exceptional circumstances for retaining certain data for longer than the normal period?	No	No further actions identified.
	12. How will information be fully anonymised or destroyed after it is no longer necessary?	Contact information will be deleted from database in line with answer to question 10.	
Principle 6 - Appropriate technical and organisation	13. What procedures are in place to ensure that all staff with access to the information have adequate information governance training?	Staff who have access to and handle personal information will need to have completed the relevant data training	Ensure that all staff have completed the relevant data training.

		Contracts with third parties include relevant clauses in relation to the handling of personal information on our behalf. All third parties, with the exception of Mail Chimp, are within the UK/EU and subject to the same data protection rules and requirements. Mail Chimp is a recognised and well established mailing list provider, used by many companies within the UK/EU.	Ensure that privacy policy includes the relevant clauses regarding information being processed outside of the EU.  Ensure that Mail Chimp is a member of the EU-US Privacy Shield.
	14. If you are using an electronic system to process the information, what security measures are in place?	All systems have access control with username / password. Only required users will have access.	No further actions identified.
	15. How will the information be provided, collated and used?	Information will be provided through the running of the website: <ul style="list-style-type: none"> <li>• Analytics information collected as users browse the website.</li> <li>• Email addresses for newsletter collected on newsletter sign up is it clear that adding an email address signs you up a news letter</li> <li>• Account information created when user creates a new account.</li> </ul>	HELM to ensure: (a) that the website enquiry form includes an option to opt out of marketing communications; (b) marketing is restricted to similar services to comply with the principles of soft opt in.
	16. What security measures will be used to transfer the identifiable information?	Information is transferred between hosted website, Mail Chip and other data providers through secure transfers.	No further actions identified.

Rights of Data Subjects			
To make information available	17. How will the organisations involved ensure that data subjects are appropriately informed of how their information will be used as part of this new process/system/service and check that current privacy notices are sufficient?	Our privacy notice refers to our partners and their privacy notices. Where there is a significant change to the privacy notice of one of our providers, consideration will be made on whether this constitutes a significant change which needs to be made aware to our data subjects.	No further actions identified.
Rights of access/data portability	18. How will you action requests from individuals (or someone acting on their behalf) for access to their personal information once held and ensure that this data is available in an easily portable format for transfer to individuals?	A listing of all systems utilised is held. In the event of such a request being made, all third party providers will be reviewed as necessary for further actions to be taken.	No further actions identified.
Rights to rectification, erasure or restriction	19. How will you action requests from individuals (or someone acting on their behalf) for their data to be rectified, erased or restricted once held?	A listing of all systems utilised is held. In the event of such a request being made, all third party providers will be reviewed as necessary for further actions to be taken.	No further actions identified.
Right to object to automated decision making	20. Will profiling or automated decision making be involved in the new system/services/process and if so, how will individuals be made aware of this and given the right to object to this?	no	No further actions identified.
Right to complain	21. How will you ensure that individuals understand that they have a right to complain about how their information is being used as part of this new project/system/service?	In the privacy policy	No further actions identified.
Other aspects of Data Protection Law			
Transfers both internal and	22. Will individual's personal information be disclosed internally/externally in identifiable form and if so to who, how and why?	no	No further actions identified.

	23. Have data controller and data processor responsibilities been clearly established between information sharing partners and key responsibilities under GDPR/DP Act documented via appropriate agreements?	<p>Contracts with third parties include relevant clauses in relation to the handling of personal information on our behalf. All third parties, with the exception of Mail Chimp, are within the EU and subject to the same data protection rules and requirements. Mail Chimp is a recognised and well established mailing list provider, used by many companies within the UK and EU.</p> <p>Staff who have access to and handle personal information will need to have completed the relevant data training</p>	Refer to question 13. No further actions identified.
	24. Will personal data be transferred to a country outside of the United Kingdom? If yes, what arrangements will be in place to safeguard the personal data?	Mail Chimp will be utilised to provide Mailing List services. Mail Chimp is a recognised and well established mailing list provider, used by many companies within the EU.	HELM to provide copies of contract and data protection arrangements to David Hankin to review.
Profiling/Automated Decision Making	25. Is any automated processing taking place to analyse individuals or predict their behaviour? If so, have they been effectively informed of this processing and the right to object to this?	No	No further actions identified.
Accountability	26. What further accountability structures or roles need to be established to support privacy within this new project/programme e.g. DPO, IAO, IG roles	None	No further actions identified.
	27. Are all parties involved in data sharing aspects of this work registered with the ICO where appropriate?	Refer to comments above. All parties are UK/EU based with the exception of Mail Chimp, based in the USA. Considerations regarding this are documented above.	No further actions identified.

Breach notification	28. Will this new process/system/service impact on the ability to report data breaches to the relevant bodies including the ICO and data subjects as appropriate?	No impact identified	No further actions identified.
Consultation needed with ICO prior to processing?	29. Could this new process/system/service result in a high risk to the rights and freedoms of individuals (in the absence of measures to mitigate the risk) and if so has the ICO been informed prior to any processing occurring?	No	No further actions identified.
Consultation	30. Who should you consult to identify the privacy risks and how will you do this? Identify both internal and external stakeholders and consider how data subjects might be included in this consultation <i>Link back to stakeholders on page 3.</i>	Discussed at length internally. Discussed with Mayfly as website designers who are used to operating in this field.  Considered each third party and relevant privacy considerations of each to assess if concerns arise. No issues noted.	No further actions identified.
	31. 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.	None in addition to the risks/concerns detailed in this report.	No further actions identified.
Other related legislation	32. Have impacts of other related legislation/codes of conduct been considered in line with the requirements of this project/system/services e.g. Privacy and Electronics Communication Regulations, Direct Marketing Code of Practice, CCTV Code of Practice etc.	No further considerations regarding privacy considered relevant to being documented here.	No further actions identified.
Guidance used	33. List any national guidance applicable to the initiative that is referred to	No specific guidance to refer.	No further actions identified.

## Section 4 - Privacy issues identified and risk analysis

Ref No.	Risk - taken into account risk to individuals, compliance risk and organisation/corporate risk	Initial Risk score - see Appendix 2			Proposed solution(s) /mitigating action(s)	Action Lead	Status/Progress	Current RAG status
		Likelihood	Impact	RAG status				
1	Transfers of data to Mail Chimp not complying with GDPR.	1	4		We will ensure that Mail Chimp, as a US company, has the appropriate privacy policy in place.	AB/DH	Reviewed privacy policies of Mail Chimp. Specifically refer to:  <a href="https://mailchimp.com/help/mailchimp-european-data-transfers/#:~:text=If%20you%20are%20a%20user,transfer%20European%20personal%20data%20to">https://mailchimp.com/help/mailchimp-european-data-transfers/#:~:text=If%20you%20are%20a%20user,transfer%20European%20personal%20data%20to</a>	Risk reduced to an acceptable level
2	Data breaches and security	2	3		Access to any system containing personal information will be limited to those users who require access to such information.  Any data downloaded from the relevant systems (which may include personal information), will only include the relevant data.  All staff with access to such data will be included on the Group's data controllers' training programme.	AB/DH	To confirm all users have received the appropriate data training.	Risk reduced to an acceptable level after training completed.

## Appendix 1: Risk Register Rating System

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 probably will 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.

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