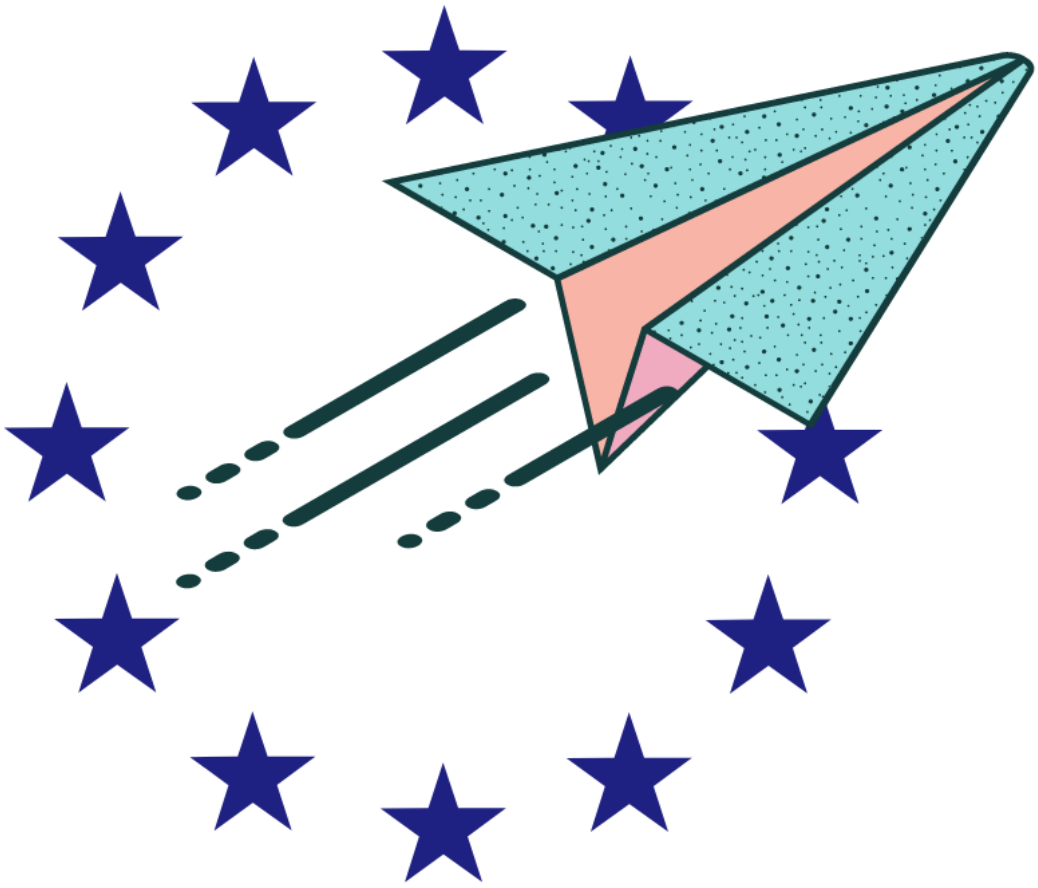

GDPR4Startups

Appendix A: GDPR4Startups Privacy Policy Template

Name of the Document	Privacy Policy
Maintained by	
Release date	

Revision History

Sr. No.	Version	Description of Change	Author	Reviewed By	Approved By	Date of Revision

Table of Contents

1. Scope

This policy applies to XYZ that is acting as a data controller for the following personal data processing activities.

A. …
B. …

2. Statement

XYZ confirms that the following sections give the best possible details of privacy policy for above mentioned personal data processing activities.

3. Policy

The following two clauses and related criteria present privacy policy for personal data processing activities mentioned in section 1.

A. Accountability: The following are the criteria relevant to how an entity manages personal data protection concerns from a governance point of view to ensure its management can assume accountability.

   a. *Policies and procedures*: XYZ has implemented the following measures that

ensure authorized management is informed, involved and accountable of personal data processing activities mentioned in section 1.

i. …
ii. …

b. *Register of processing activities*: XYZ's management reviews and approves on a regular basis, see schedule below, the register of the personal data processing activities under its responsibility to ensure completeness and accuracy of the record.

i. …
ii. …

c. *Data protection officer (DPO)*: XYZ has assessed requirements to designate a Data Protection Officer (DPO) and has taken the following actions.

i. …
ii. …

d. *Data breach*: XYZ has implemented the following technical and organizational measures to effectively detect, manage and if applicable notify personal data breaches to concerning parties (data subject and supervisory authority).

i. …
ii. …

B. Principles Relating to Processing of Personal Data (Controller): The following are the criteria relevant to how an entity manages personal data protection requirements for a given processing activity in scope, where it acts as controller.

a. *Lawfulness*: XYZ has implemented the following measures to ensure that a valid legal basis is identified for each processing activity mentioned in section 1.

i. …
ii. …

b. *Transparency:* XYZ has also implemented measures to ensure that the data subject is provided with the following information at the time when personal data is obtained/collected.

i. How do we collect your personal data?

Example: You directly provide XYZ with most of the data we collect. We

collect data and process data when you:

- *Register online or place an order for any of our products or services.*
- *Voluntarily complete a customer survey or provide feedback on any of our message boards or via email.*
- *Use or view our website via your browser's cookies.*
- *[Add any other ways your company collects data]*

XYZ may also receive your data indirectly from the following sources:

- *[Add any indirect source of data your company has]*

ii. How do we process your personal data?

Example: XYZ collects your data so that we can:

- *Process your order and manage your account.*
- *Email you with special offers on other products and services we think you might like.*
- *[Add how else your company uses data]*

iii. On what legal ground(s) do we process your personal data

iv. Which personal data do we collect and further process?

Example: XYZ collects the following personal data:
Name, email address, phone number
[Add any other data your company collects]

v. How long do we keep your personal data?

Example: XYZ will keep your [enter type of data] for [enter time period]. Once this time period has expired, we will delete your data by [enter how you delete users' data].

vi. How do we protect and safeguard your personal data?

Example: XYZ securely stores your data at [enter the location and describe security precautions taken i.e. ISO27001 measures you or your

service provider have implemented, see previous section].

vii. Who has access to your personal data and to whom is it disclosed?

Example: XYZ will share your data with the following departments so that we offer you requested products and services.

- *[List departments that will receive data]*

If you agree, XYZ will share your data with our partner companies so that they may offer you their products and services.

- *[List organizations that will receive data]*

When XYZ processes your order, it may send your data to, and also use the resulting information from, credit reference agencies to prevent fraudulent purchases.

viii. What are your rights and how can you exercise them?

Example: XYZ would like to make sure you are fully aware of all of the following data protection rights.

The right to access – You have the right to request *XYZ* for copies of your personal data. We may charge you a small fee for this service.

The right to rectification – You have the right to request that *XYZ* correct any information you believe is inaccurate. You also have the right to request *XYZ* to complete the information you believe is incomplete.

The right to erasure – You have the right to request that *XYZ* erase your personal data, under certain conditions.

The right to restrict processing – You have the right to request that *XYZ* restrict the processing of your personal data, under certain conditions.

The right to object to processing – You have the right to object to *XYZ*'s processing of your personal data, under certain conditions.

The right to data portability – You have the right to request that *XYZ* transfer the data that we have collected to another organization, or directly to you, under certain conditions.

If you make a request, we have one month to respond to you. If you would like to exercise any of these rights, please contact us at our email:

Call us at:

Or write to us:

ix. How to contact us?

Example: If you have any questions about XYZ's privacy policy, the data we hold on you, or you would like to exercise one of your data protection rights, please do not hesitate to contact us. *Email us at:* *Call us:* *Or write to us at:*

x. How to contact the appropriate authorities?

Example: Should you wish to report a complaint or if you feel that XYZ has not addressed your concern in a satisfactory manner, you may contact the Information Commissioner's Office. *Email:* *Address:*

xi. When to expect changes in privacy policy?

Example: XYZ keeps its privacy policy under regular review and places any updates on this web page. This privacy policy was last updated on XX/XX/XXXX.

xii. Websites (if applicable)

1. What are cookies?

Example: Cookies are text files placed on your computer to collect standard Internet log information and visitor behavior information. When you visit our websites, we may collect information from you automatically through cookies or similar technology. For further information, visit allaboutcookies.org.

2. How do we use cookies?

> *Example: XYZ uses cookies in a range of ways to improve your experience on our website, including:*
> - *Keeping you signed in*
> - *Understanding how you use our website*
> - *[Add any uses your company has for cookies]*

3. What types of cookies do we use?

> *Example: There are a number of different types of cookies, however, our website uses:*
> - *Functionality – XYZ uses these cookies so that we recognize you on our website and remember your previously selected preferences. These could include what language you prefer and location you are in. A mix of first-party and third-party cookies are used.*
> - *Advertising – XYZ uses these cookies to collect information about your visit to our website, the content you viewed, the links you followed and information about your browser, device, and your IP address. XYZ sometimes shares some limited aspects of this data with third parties for advertising purposes. We may also share online data collected through cookies with our advertising partners. This means that when you visit another website, you may be shown advertising based on your browsing patterns on our website.*
> - *[Add any other types of cookies your company uses]*

4. How can you manage the cookies?

> *Example: You can set your browser not to accept cookies, and the above website tells you how to remove cookies from your browser. However, in a few cases, some of our website features may not function as a result.*

5. Privacy policies of other websites (if applicable)

> *Example: XYZ website contains links to other websites. Our privacy policy applies only to our website, so if you click on a link to another website, you should read their privacy policy.*

c. *Purpose limitations*: XYZ has implemented the following measures to ensure that it has assessed that the purpose(s) for which it collects the data are specific, explicit and legitimate.
   i. …
   ii. …

d. *Data minimization*: XYZ has implemented the following measures that ensure that the collection of personal data is limited to what is necessary in relation to the purposes for which they are processed.
   i. …
   ii. …

e. *Accuracy*: XYZ has implemented the following measures that ensure that the data sources used to collect personal data are relevant and processed data is accurate.
   i. …
   ii. …

f. *Storage limitation*: XYZ has implemented the following measures that ensure that the retention periods for processed data is defined and communicated to concerned parties.
   i. …
   ii. …

g. *Security (integrity, availability, and confidentiality)*: XYZ has implemented the following organizational and technical measures that ensure protection for processed data.
   i. … (ISO27001 measures you or your service provider have implemented, see previous section)
   ii. …

h. *Privacy by design*: XYZ has implemented the following measures that ensure that data protection principles are integrated when the personal data processing

activity mentioned is developed.

i. …
ii. …

i. *Privacy by default:* XYZ has implemented the following measures that ensure that the personal data processing activity when developed is by default set up in the most privacy friendly/preserving way for the data subjects.
   i. …
   ii. …

j. *Outsourcing*: XYZ uses a processor and has implemented the following measures to assess that the processor is providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements and ensure the protection of the rights of the data subject.
   i. …
   ii. …

k. *Exercise of rights of data subject*: XYZ has implemented the following measures to ensure exercise of the applicable rights towards data subjects (e.g. the right of access, the right of rectification, the right of opposition, the right of information, the right of portability, the right to be forgotten, and the right to contest a decision based on automated processing).
   i. …
   ii. …

l. *Transfer of personal data to third countries*: XYZ has implemented the following measures to ensure that legal safeguard has been put in place when transferring the personal data to a third country or an international organization.
   i. …
   ii. …