GDPR Checklist

This document is based on:

1. UK Information Commissioner's Office official checklist: https://ico.org.uk/for-organisations/data-protection-self-assessment/controllers-checklist/
2. Our hands-on experience.

Id	Status	Action item	□
1	Best practice	**Create an informational map of data flows.** The company should map every moment of the personal data lifecycle. The company must know what happens to personal data, why and if any external parties are used (Processors).	□
2	Best practice	**Documented what personal data the company has, where it came from, who gets this information and what to do with it.** Absolute priority in performing compliance with GDPR.	□
3	Required	**Identify lawful basis for processing of personal data. Make sure the legal basis is in place when processing personal data.** Legal obligation (Article 6), one of priorities in complying with GDPR.	□
4	Required	**Validate and update privacy policy, terms of service, employment agreements, contracts, etc… to comply with privacy requirements.** Besides those, one should implement a number of internal Codes of conduct. where internal team will know what is allowed and what is not related to personal data.	□
5	Required	**Perform due diligence to ensure that company' subcontractors or 3rd parties are GDPR compliant.** Business must have a written contract with all processing companies. DPA contracts should be signed with all suppliers, no matter if they currently have access to personal data or not; additionally every Controller should evaluate the option to use NDA in business. In terms of technical measures of personal data protection, SLA with key suppliers (Processors) should be in place as well.	□
6	Required	**Perform Data Protection Impact Assessments.** DPIA is performed when VERY sensitive data are collected and processed. Controllers should perform DPIA in order to estimate risk	□

		of sensitive data exposure and add additional methods to secure such data.	
7	Required	**Special data treatment for health data or children’s personal data, etc…** Explained in DPIA part.	□
8	Required	**Monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.** As in ISO standards, one is obliged to perform GDPR compliance audit, preferably not internally, but to have an external partner performing audit.	□
9	Best practice	**Update contracts (terms of service, privacy policy, etc…) to cover International data transfer.** This can be a part of an annual audit.	□
10	Required	**Depending on the company size you might need to hire a Data Privacy Officer (DPO).** Either related to size or (even more important) if one collects and processes VERY sensitive data - in those cases DPO MUST be appointed.	□
11	Required	**Physical and organisational security measures.** Best would be to implement ISMS (ISO 27001 - Information Security standard).	□
12	Required in some countries	**UK companies might need to register in the Information Commissioner's Office. Each country has its own local laws.** Following national and international legal framework, should be part of report when performing annual audit (input should be “what’s new” in regulations worldwide)	□
13	Required	**Data protection awareness training.** Training, education and permanent awareness on GDPR topics is obligatory, one might have to prove that it is done on a regular basis.	□
14	Required	**Data protection by design** ✓ **Databunker** can serve as a cornerstone for your privacy by design solution.	□

15	Best practice	**Personal data consolidation** ✔You can move all your personal data saved in different databases to **Databunker**.	□
`16	Best practice	**Personal data encryption & hashing.** ✔Personal data and session data saved in **Databunker** is automatically encrypted.	□
17	Best practice	**Personal data pseudonymisation.** ✔**Pseudonymisation** is a perfect solution for cross-border personal data transfer. When saving a user object in **Databunker** you are getting a user token. This user token is a user **pseudonymised identity**. When performing a cross-border transfer, change user personal data with a **Databunker user token**. ✔**Pseudonymisation** helps with storing logs: https://www.freecodecamp.org/news/how-to-stay-gdpr-compliant-with-access-logs/	□
18	Required	**Data confidentiality, integrity and availability.** ✔**Databunker** was built for this purpose. The product supports clustering and high availability. It stores an audit trail on every operation.	□
19	Required	**Data minimization** ✔You can extract not-active users from **Databunker** and remove them. ✔By consolidating personal data from different systems into **Databunker** improves data minimization.	□
20	Required	**Keep track of operations with PII.** ✔**Databunker** keeps track of every PII access and change.	□
21	Required	**Storage of legal bases (i.e. consent).** ✔**Databunker** has an API and UI to store legal bases (i.e. consent).	□
22	Best practice	**Encrypted session storage.** ✔**Databunker** has encrypted session storage built in function. Node.js example is provided.	□
23	Best practice	**Make logging GDPR ready.** ✔**Databunker** can help you here with Pseudonymisation. Follow this article:	□

		https://www.freecodecamp.org/news/how-to-stay-gdpr-compliant-with-access-logs/	
24	Feature	**Built-in node.js support.** ✓Full working example for **Databunker**: https://github.com/securitybunker/databunker-nodejs-example	□
25	Feature	**End-customer privacy portal - data subject access.** ✓**Databunker** comes with a privacy portal. Your customers can perform data subject requests inside the tool.	□
26	Required	**Your business need to be ready to comply with the following user rights:** ● User right of access ● User right to be informed ● User right of correction ("rectification") ● User right of erasure ● User right to restrict processing ● User right of data portability ● User right related to automated decision making including profiling ● User right to object ✓You must update your privacy policy and add an email of the DPO or a lawyer who will execute user requests. ✓You need to create a checklist for the commands to do to serve customer requests or you can use **Databunker** for automation. ✓**Databunker** has a self-service privacy portal. You can add a link to the portal in the privacy policy.	□
27	Required	**DPO: Data Subject Request management and execution.** ✓**Databunker** has a user interface for the DPO to manage user requests for internal data. ✓**PrivacyBunker.io** SaaS has a UI for the DPO to manage user requests for user records stored in different databases or in SaaS companies. ✓**DatabunkerPro** has a combination of both tools.	□
28	Required	**Data removal or anonymization for deactivated or expired accounts. (Data minimization)** ✓**Databunker** has an API for that for internal data. ✓**PrivacyBunker.io** SaaS can help you with data stored in external databases or SaaS companies. ✓**DatabunkerPro** has a combination of both tools.	□
29	Required	**Execute Data Subject forget-me request.** ✓**Databunker** has a UI and an API for that for internal data. ✓**PrivacyBunker.io** SaaS can remove personal data stored in	□

		external databases or SaaS companies. ✓**DatabunkerPro** has a combination of both tools.	
30	Feature	**Personal data report generation using SaaS and DB connectors for the end customer and for DPO.** ✓**PrivacyBunker.io** SaaS is our additional service that can be used for that. ✓**DatabunkerPro** has the same functionality.	□
31	Required	**Built-in cookie consent popup.** ✓**PrivacyBunker.io** SaaS is our additional service that can be used for that. ✓**DatabunkerPro** has the same functionality.	□
32	Required	**Reporting breaches in 72 hours.** ✓Our support will provide you templates for reporting.	□
33	Feature	**Unstructured files scanning.** Depending on your situation, to stand your customer privacy rights, you might need to lookup user records in unstructured files. You will need to create special scripts for that.	□

For more info:

1. https://databunker.org/ Databunker project.
2. https://databunker.org/files/presentation.pdf Databunker presentation.
3. https://privacybunker.io/ Privacybunker SAAS.

Node.js support

- Databunker example with Passport.js and Magic.Link https://github.com/securitybunker/databunker-nodejs-example
- Databunker personal data store Node.js module https://www.npmjs.com/package/@databunker/store
- Databunker secure session store Node.js module https://www.npmjs.com/package/@databunker/session-store

Questions?

For any questions and support requests mail us at yuli@privacybunker.io