BEEKEEPER

White Paper

YOUR 31-POINT ASSESSMENT TO ENSURE GDPR COMPLIANCE

INTRODUCTION

The EU General Data Protection Regulation (GDPR) was designed to harmonize data privacy laws across Europe to protect citizens' personal data and stand on a united front regarding every organization's approach to security. It was approved on April 14, 2016 and will be enforced May 25, 2018. Any companies that aren't compliant will face heavy fines up to 4% of annual global turnover or $20 million Euros, whichever is greater.

If you work for a North American Company, you may think this doesn't affect your data security standards—but think again. The GDPR doesn't only affect companies in the EU. Any vendors and suppliers that work with countries in the EU must comply with the GDPR as well. Now is the time to assess your GDPR compliance and see what extra steps your organization needs to take to meet the deadline.

31-POINT ASSESSMENT

We've compiled a list of 31 questions to ask of your Company to start the process of being GDPR compliant.

1. Does your Company process Personal Data in an EU country or of EU residents? (Personal Data is any data that may be used to identify a person, including technical, genetic, cultural, mental, economic, and social information.) ☐

2. Is your Company familiar or registered with the EU-US Privacy Shield Framework (https://www.privacyshield.gov/welcome)? ☐

3. Does your Company utilize technology to detect and alert a data breach (IDS / HIDS)? ☐

4. Does your Company maintain an inventory of all Assets which process (transfer / store) Personal Data? ☐

5. Are your Company's Personal Data Flow channels identified? ☐

6. Is your Company technically equipped to search for and permanently remove one individual's Personal Data? ☐

7. Is the concept of "Privacy by Design" incorporated in your Personal Data processing products and services? ☐

8. Do you apply a Privacy Impact Assessment in your product or service development lifecycle? ☐

9. Is permanent deletion of Personal Data according to a standard such as NIST (or other)? ☐

10. Does your Company have direct access to all the systems used for their processing of Personal Data? ☐

11. Does your Company have a Right to Audit all the systems used for their processing of Personal Data? ☐

12. If your Company transfers Personal Data to a Third Party Company, is this transfer governed under a Data Protection Agreement? ☐

13. Does your Company only retain Personal Data for the minimum period that is required for the purpose that it was obtained? ☐

14. Is Personal Data encrypted or anonymized or pseudonymised for long-term storage (backup systems, tape, etc.) ☐

15. Is access to Personal Data based on the "Need to Do---Need to Access" principle? ☐

16. Is the level of protection of Personal Data the same across the Company and any relevant Third Party Company environment? ☐

17. Is access to Personal Data controlled by both Authentication as well as Authorization technologies and respective processes? ☐

18. Do you maintain auditability over the full Personal Data lifecycle your Company processes? ☐

19. Does your Company avoid profiling based on Personal Data for decision making purposes relevant to performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location, or movements? ☐

20. Are all of the following factors true when obtaining Consent from a Data Subject: ☐

(a) Purpose for consent is communicated, clear, and transparent
(b) Consent given is not based on silence or inactivity or pre-checked boxes
(c) Consent obtaining process is available and auditable
(d) Consent may be revoked easily

21. Does your Company have a defined Data Breach Notification process, meeting the requirements identified in Articles 33, 34 of the General Data Protection Regulation? ☐

22. Does your Company follow a Data Minimization strategy? ☐

23. Does your Company avoid manual processing of Personal Data? ☐

24. Does your Company generate aggregate Data which is sanitized from any Personal Data? ☐

25. Does your Company process Personal Data in other jurisdictions which meet the following: ☐
(a) The other jurisdiction legal framework ensures an adequate level of protection for Personal Data
(b) The Personal Data transfer is subject to appropriate technical safeguards
(c) There is a contractual binding between the sender and receiver of Personal Data

26. Has your Company appointed a DPO (Data Protection/Privacy Officer)? ☐

27. Does your Company avoid using Personal Data for purposes other than what was communicated to the Data Subject? This includes for general testing purposes, transfer to an affiliated Company not in the original purpose under which the Personal Data was originally collected, or for marketing purposes not consented to explicitly by the Data Subject. ☐

28. Is your Company's Privacy Policy transparent and clear about processing of Personal Data? ☐

29. Does your Company provide employees working with Personal Data regular training on handling Personal Data? ☐

30. Is your Company aware of the sensitivity rating of Personal Data for ages up to 16? ☐

31. Do you systematically maintain a list of all Third Party Companies who receive Personal Data from your Company (whether directly or indirectly)? ☐

Disclaimer: These are the questions that Beekeeper has been using internally to assess compliance and, at the request of many colleagues, our CISO has been asked for his recommendations. These are not sanctioned by GDPR. For the full GDPR requirements visit:

Official EU Documentation: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1499864717744&uri=LEGISSUM:310401_2

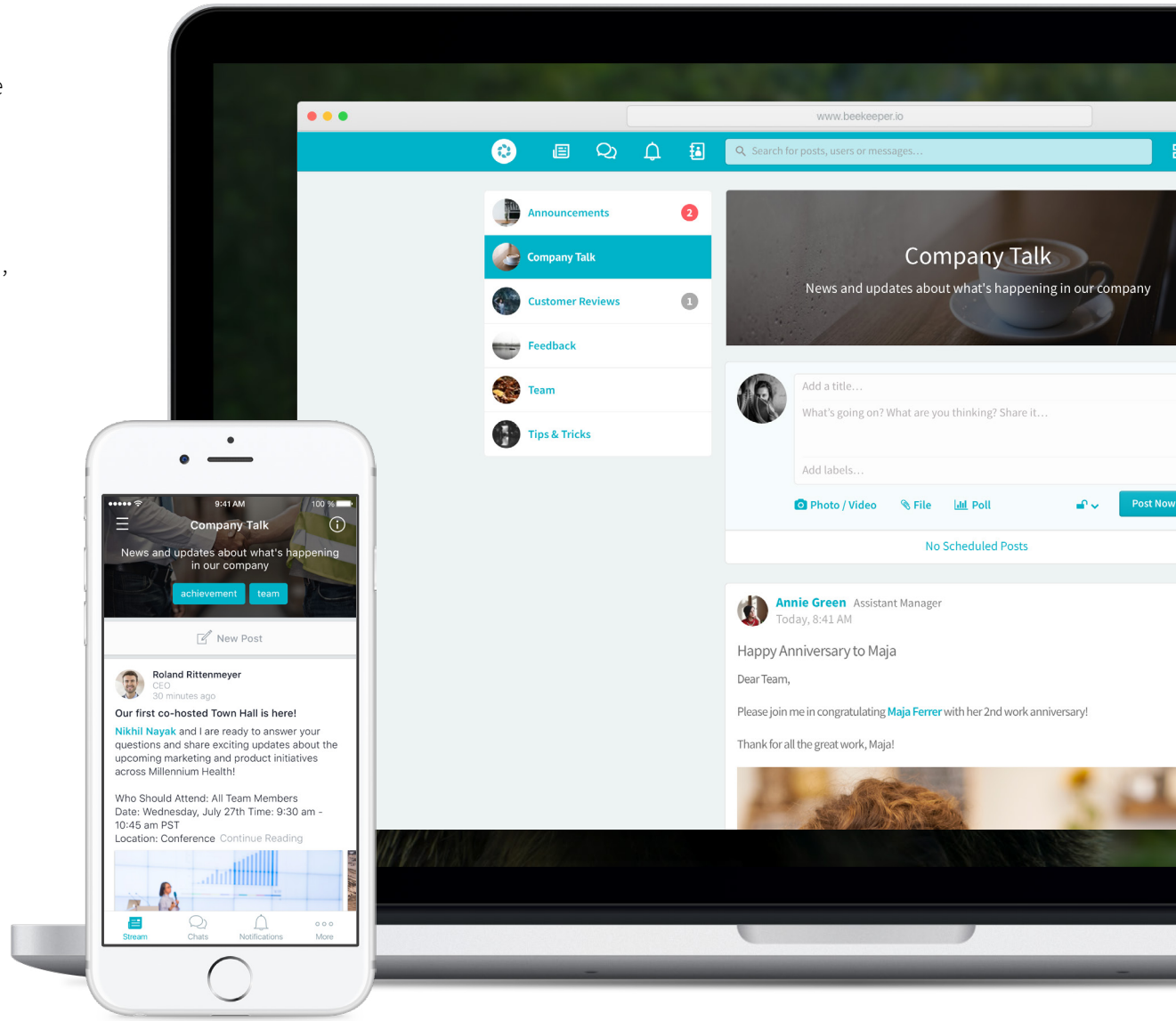
Documentation Online:
https://gdpr-info.eu/

Official Archive:
http://ec.europa.eu/justice/data-protection/

Unofficial:
http://www.eugdpr.org/eugdpr.org.html

BEEKEEPER

Beekeeper is an award-winning digital workplace app that digitizes the non-desk workforce by connecting operational systems and communication channels within one secure, intuitive platform. Beekeeper connects colleagues across locations and departments in real time via mobile or desktop devices, and includes an intelligent dashboard to help companies improve internal communication and streamline business processes. Secure, automated, and relevant information is readily distributed, searchable, and measurable in one central hub for an efficient digitized workflow. The company is based in Zurich and San Francisco and supports users in more than 130 countries.



For more information, visit www.beekeeper.io and follow us @BeekeeperSocial.