How IT Managers Can Help Their Legal Teams Prepare for the GDPR

The General Data Protection Regulation ("GDPR") is changing the way organisations handle personal data. The GDPR introduces new laws that will require process changes and tightening of data security for many organisations.

As the leader in Cloud Identity, Okta has outlined some key points for IT managers to prepare their organisation's legal team to help ensure GDPR compliance. This checklist is simply a starting point for helping your organisation map out organisational structures and coordinate internal stakeholder teams. Using this checklist in conjunction with a comprehensive identity access management product is a step in ensuring that your organisation is prepared for the GDPR before it rolls out in 2018.

For legal advice regarding your organisation's GDPR compliance needs, be sure to consult your organisation's lawyer. This sample checklist does not constitute legal advice and is provided for informational purposes only.

User Data

1. **The number of European individuals you have collected personal data from**

   The GDPR only applies to organisations that collect, process, and store personal data from European Union (EU) individuals.

2. **Whether your organisation collects, processes, or stores information about EU children**

   The GDPR has special rules concerning the data of children and requires parental consent for data to be obtained for children ranging from 13 to 16 years old, depending on the member's state.

3. **Whether the personal data of EU individuals is pseudonymous or encrypted**

   Although pseudonymous or encrypted data is not exempt from the law, the GDPR relaxes several requirements on controllers that apply this technique to the personal data they collect, process, or store.

4. **Any processing of sensitive data**

   Is your organisation collecting, processing, or storing any sensitive personal data (race or ethnic origins; political opinions; religious or philosophical beliefs; sex life and sexual orientation; genetic, biometric, or health data; criminal convictions; trade union membership) and are you doing so on appropriate grounds?

5. **Specific information about all personal data subject to the GDPR, including:**

   What employees have access to what personal data.

   Which data subjects have given consent and whether you are currently using the data in accordance with this consent.

   Commonly used formats in which data is kept (the GDPR requires that personal data be portable and in an open standard electronic format).

Company Personnel

6. **Whether you are a data controller or data processor for each type of personal data subject to the GDPR**

   Whether you're in control of the data or acting at the direction of another is crucial to understanding what is required of your organisation by the GDPR.

7. **Data Protection Officer**

   Is a Data Protection Officer in place or does one need to be appointed to comply with the GDPR, based on your organisation's activities?

8. **Processors and sub-processors**

   Is there written documentation in place about the relationship and responsibilities of processors and sub-processors that handle personal data?

   Do you have a full list of sub-processors for the personal data you handle?

Records and Contracts

9. **Prepare detailed records of processing activities**

   Organisations subject to the GDPR and that are properly categorized as controllers must keep records of their processing activities, and be prepared to disclose these records to Data Protection Authorities if requested.

10. **Identify and review all relevant contracts**

    New contracts may need to be reviewed for customer and third-party vendor agreements. Additionally, your organisation's current contracts that are subject to GDPR considerations may need to be revised to ensure compliance with the GDPR.

Logistics and Plans

11. **Information about technical and operational processes**

    Removal of personal data is an auditable activity by Data Protection Authorities, so ensure your organisation has a process in place for granting data subject access or deletion requests. This will help ensure compliance with the GDPR's provisions about data subjects' right to erasure and right to data portability.

12. **A privacy governance model**

    This should clearly show roles and responsibilities within the enterprise and how data breaches are to be reported. Have staff been trained on new processes and regulations?

13. **Privacy by design strategies**

    The GDPR requires that privacy be considered in all major IT decisions to ensure data minimisation and security.

14. **Data export mechanisms**

    The GDPR only allows for data to be exported out of the European Economic Area if the importing country offers adequate protections for the data. Work with your organisation's legal team to ensure these lawful transfer mechanisms are properly accounted for.

15. **A data breach response plan**

    The GDPR requires organisations to act quickly and notify the affected data subjects where necessary.

Identity and Access Management (IAM) Strategy

A critical step in achieving GDPR compliance is having a documented IAM strategy that identifies what data you're collecting and where its located. The following tools benefit both IT and legal teams by providing transparency, security, and visibility into this data:

16. **Universal Directory**

    Can your legal team easily find users in the enterprise and see which applications they have access to? Universal Directory offers the ability to easily identify and manage individual users, including removing users (and their personal data) if necessary.

17. **Single Sign-On (SSO)**

    With Okta SSO your team can reduce identity sprawl and obtain a single source of truth for right-to-be-forgotten deletion requests.

18. **Adaptive Multi-Factor Authentication (MFA)**

    With Okta's AMFA, your legal team can rest assured about the security of your organisation's most sensitive data and create robust access policies based on user data such as location, IP address, or device.

This checklist provides a basis for the type of information that you may want to share with your legal team as your organisation prepares for the GDPR. We've also created a GDPR White Paper, where you can learn more about the requirements of the GDPR and how Okta can help your organisation stay ahead of the changes.

Are you looking for more clarity on specific GDPR terms?
Okta's GDPR glossary will keep you informed.

About Okta

Okta is the leading provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 5,000 apps, the Okta Identity Cloud enables simple and secure access from any device.

Thousands of customers, including Experian, 20th Century Fox, LinkedIn, Flex, News Corp, Dish Networks and Adobe trust Okta to work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

okta.com