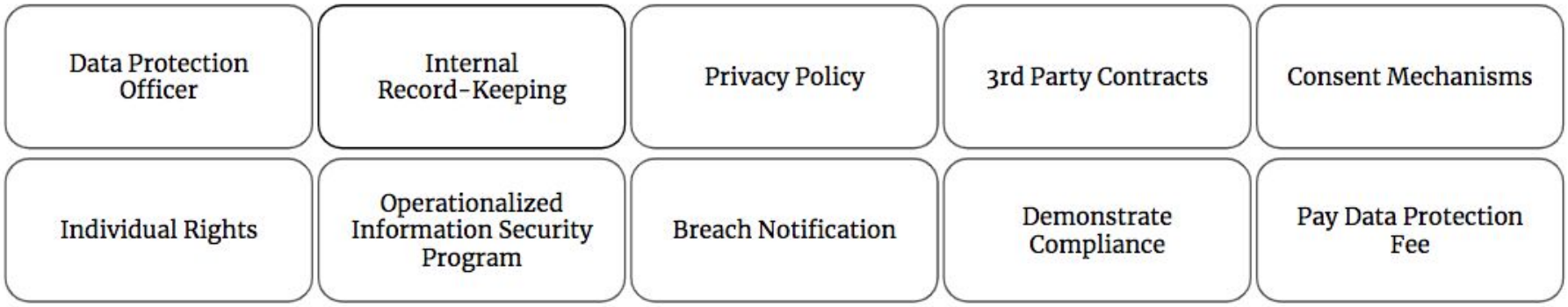
The 10 GDPR Components

GDPR Stand Up

Overview

GDPR can be broken down into the following 10 components. Some companies will need to fulfill all components, while others will only need to fulfill some. This all depends on the data your company holds. More specifically, it depends on the type of data your company holds, how the data is obtained, and how the data is used.



© 2018 CyberSecurityBase, Inc

The 10 GDPR Components

GDPR Stand Up

Quick Reference Guide

Component	Description
Data Protection Officer	An appointed individual that owns and manages data protection responsibilities.
Internal Record-Keeping	Documentation of your data management practices, which primarily determine the scope of your GDPR responsibilities.
Privacy Policy	A public-facing notice (or set of notices) describing your data management practices.
3rd Party Contracts	Written agreements with 3rd parties that you exchange personal data with.
Consent Mechanisms	A system of features and processes to manage consents on how your company (and in some cases 3rd parties) can use an individual's personal data.
Individual Rights ● Access Rights (SARs) ● Corrections Rights ● Erasure Rights ● Restrict Processing Rights ● Data Portability Rights ● Objections Rights ● Automated-Decision Making Rights	A set of features and processes that will provide individuals with rights afforded by GDPR, with respect to the use of personal data held about them. ● **Access:** Requests to access personal data you hold about an individual ● **Corrections:** Requests to review and correct personal data you hold about an individual ● **Erasure/Right to be Forgotten:** Requests to delete personal data of an individual ● **Restrict Processing:** Requests to change how your company can use an individual's personal data ● **Data Portability:** Requests to obtain personal data from your company and extract for purposes of using across different services ● **Objections:** Requests to object to how your company can use an individual's personal data ● **Automated-Decision Making:** Requests related to using personal data to profile an individual and/or make an automated decision
Operationalized Information Security Program	A collection of activities and practices geared to protect personal data. This includes a collection of activities that define information security requirements and supporting activities to operationalize that across the company. ● Policy: Defines company-wide security requirements ● Training: Educates employees and contractors of the relevant security requirements ● Processes: Operationalizes security requirements into day-to-day business processes
Breach Notification	Reporting of personal data breaches to supervisory authorities (i.e. regulators) and/or affected individuals. This includes internal capabilities to monitor, detect, review, document, and notify about personal data breaches.
Demonstrate Compliance	Internal governance structure to demonstrate GDPR compliance. This includes performing reviews and maintaining records of these governance measures.
Pay Data Protection Fee	A fee to ensure continued funding of the Information Commissioner's Office (ICO).