msgGillardon

Die neue EU-Datenschutzgrundverordnung

Herausforderungen und Lösungen

Mit Umsetzung der neuen EU-Datenschutzgrundverordnung (EU-DSGVO) sollen Banken ein verbessertes Datenschutzniveau bei der Verarbeitung personenbezogener Daten sicherstellen. Die Umsetzung der neuen Vorgaben der EU-DSGVO ist mit Augenmaß vorzunehmen, um auf der einen Seite unnötigen Aufwand für Ihr Haus zu vermeiden. Auf der anderen Seite ist zu berücksichtigen, dass Verstöße gegen die EU-DSGVO mit Geldbußen von bis zu 4 Prozent der weltweit erzielten Jahresumsätze geahndet werden können.

Die EU-DSGVO sieht vor allem folgende Neuerungen vor:

- Verschärfte Anforderungen an eine Risikoanalyse zur Datenschutzfolgeabschätzung.
- Erweiterte Informations- und Hinweispflichten an Kunden.
- Neue Anforderungen an die Einwilligungserklärungen durch Kunden.
- Neue Anforderungen an die Auftragsverarbeitung durch Dritte.
- Erweiterte Betroffenenrechte, wie zum Beispiel Recht auf Datenportabilität und Recht auf Vergessenwerden.
- Neue Anforderungen an das Verfahrensverzeichnis.
- Erweiterte Sanktionsmöglichkeiten sowie massiv gestiegene Haftungsrisiken.
- Neue Fristen und Transparenzpflichten.
- Verschärfte Notifikationspflichten bei Datenschutzverstößen (data breach).
- Neue und verschärfte Anforderungen an IT-Umgebung (privacy by design/privacy by default).

Alle Neuerungen und umzusetzenden Maßnahmen müssen an den folgenden, in der EU-DSGVO festgelegten Grundsätzen der Verarbeitung personenbezogener Daten ausgerichtet werden: Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, Rechenschaftspflicht.

Herausforderungen

- Die Umsetzungsfrist der neuen Anforderungen aus der DSGVO für die betroffenen Institute ist bis zum 25. Mai 2018 knapp bemessen.
- Die datenschutzrechtlichen Anforderungen umfassen verschiedene Geschäftsbereiche, IT-Anwendungen, Prozesse sowie eine Vielzahl von unterschiedlichen Arten von Formularen und Verträgen.
- Das Zusammenspiel von IT-Anwendungen und Prozessen (inklusive Anweisungen und Dokumenten) muss in einer übergeordneten Datenschutzorganisation optimal und stringent aufeinander abgestimmt und Verantwortungsbereiche klar definiert werden.
- Die Rechtmäßigkeit der Datenverarbeitung muss für alle Bereiche sichergestellt werden. Daher ist mitunter von Fall zu Fall eine neue Bewertung erforderlich.
- Die Neuerungen aus der DSGVO müssen den relevanten Mitarbeitern in der Bank zeitnah vermittelt werden.

Unser Vorgehensmodell – wesentliche Handlungsfelder

Wir richten unser Vorgehensmodell an Ihren Vorstellungen beziehungsweise an der konkreten Situation Ihres Hauses aus. Dabei bringen wir unsere umfassende IT- und Fachkompetenz aus einer Vielzahl von Projekten zum Datenschutz mit ein. Insbesondere sehen wir folgende Handlungsfelder:

1 Datenschutzorganisation
- Identifizierung betroffener Abteilungen, Prozesse und Formulare und Verträge.
- Umsetzung der Anforderungen an Löschung, Berichtigung sowie Übertragbarkeit von Daten
- Ableiten und Umsetzen der Maßnahmen

2 Datenschutzfolgeabschätzung
- Neue Positiv- und Negativ-Listen der DSGVO zur Folgenabschätzung sind institutsspezifisch zu berücksichtigen.
- Implementierung Prozess zur Konsultationspflicht gegenüber Aufsichtsbehörde

3 Auftragsdatenverarbeitung
- Sämtliche neuen Inhalte der DSGVO (Scoring, Auskunfteien, etc.) sind in den Verträgen mit Auftragsverarbeitern zu berücksichtigen.
- Neue Standard-Musterverträge sind angekündigt

4 Formulare und Dokumente (Kunden)
- Sämtliche internen und externen Formulare und Verträge sind auf eine mögliche Betroffenheit hin zu untersuchen.
- Anpassungsbedarf ist systematisch zu dokumentieren und umzusetzen.

5 Einwilligungserklärungen
- Bestehende Einwilligungserklärungen sind zu identifizieren bzw. zu klassifizieren.
- Anpassungsbedarf ist mit Rechtsabteilung bzw. Datenschutzbeauftragtem abzustimmen und mit Kunden neu zu vereinbaren.

6 Schulung betroffener Abteilungen
- Betroffene Prozesse und Mitarbeiter sind zu identifizieren.
- Die veränderten regulatorischen Anforderungen sind zu vermitteln und der korrekte Umgang damit sicherzustellen.

IT-Anwendungen (Berechtigungs-, Notfall- und IT-Konzepte) privacy by design & default

Warum msgGillardon?

- Wir stellen Ihnen ein interdisziplinär aufgestelltes Team zur Verfügung, das über langjährige Erfahrungen in den Bereichen Datenschutz, IT- Sicherheit und Revision verfügt.
- Wir setzen auf den bei Ihnen bereits vorhandenen Strukturen auf und entwickeln gemeinsam mit Ihnen passgenaue Lösungen für Ihr Institut.
- Unsere Teammitglieder verfügen über umfassenden juristischen und prüferischen Sachverstand, so dass die Angemessenheit von Dokumenten, Verfahren und Vertragsgestaltungen adäquat nachvollzogen und sichergestellt werden kann.
- Wir verwenden vielfach erprobte Excel-Tools zur effizienten Bestandsaufnahme sowie zur Dokumentation und zum Monitoring der abgeleiteten Maßnahmen.
- Wir vermeiden ein Over-Engineering und stellen damit auch sicher, dass Sie die Tools und Ergebnisse auch für die Zukunft weiterverwenden können.

Ihre Ansprechpartner

Alexander Nölle
alexander.noelle@msg-gillardon.de

Andreas von Heymann
andreas.von.heymann@msg-gillardon.de

Christoph Prellwitz
christoph.prellwitz@msg-gillardon.de

T-440-SL-12 17-1