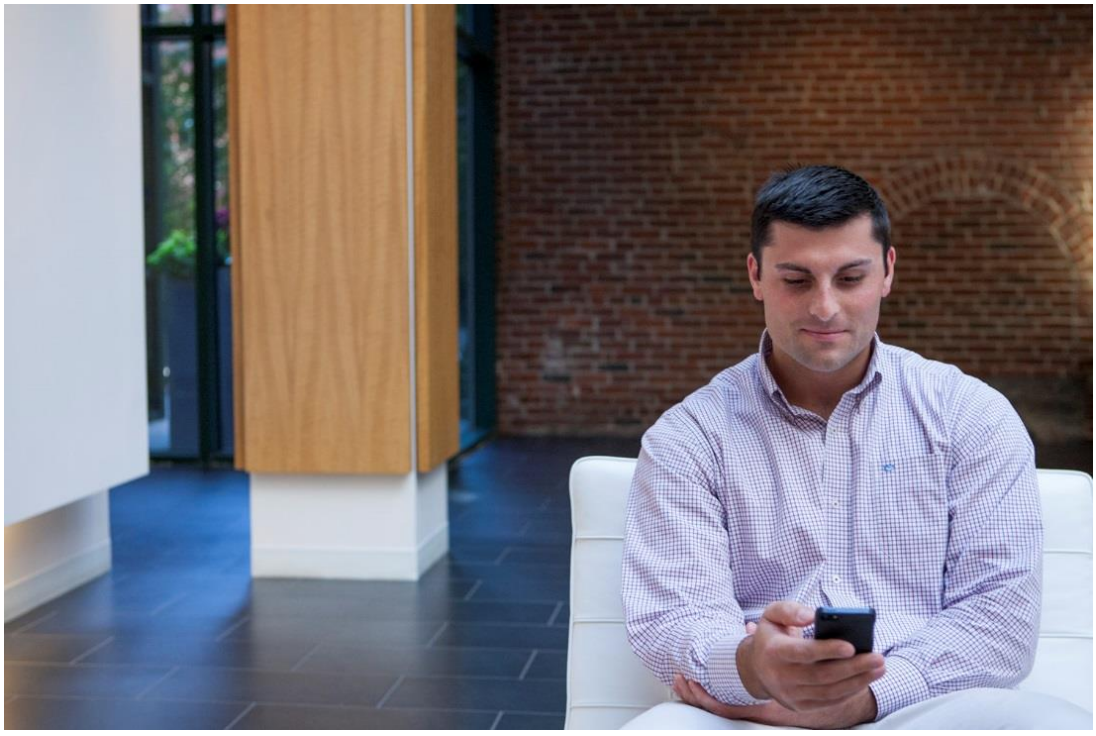
DSGVO

Technik und Sicherheit der Datenverarbeitung

Klaus Rathsfeld
Annett Hänel

Inhalt



DSGVO gilt ab 25.05.2018 in der gesamten Europäischen Union

Am 25. Mai 2018 tritt die europaweit gültige Datenschutz-Grundverordnung (DSGVO) in allen Ländern der Europäischen Union in Kraft und ersetzt in Deutschland das bisher gültige Bundesdatenschutzgesetz. Aus diesem Grund haben wir gemeinsam mit unserem internen Datenschutzbeauftragten ein E-Book entwickelt, das Ihnen die zentralen Inhalte und Veränderungen übersichtlich und so kurz wie möglich darstellen soll.

Die DSGVO stellt die Rechte und Freiheiten der betroffenen Personen – also derjenigen, deren personenbezogene Daten verarbeitet werden – in den Vordergrund und schreibt die bisherigen datenschutzrechtlichen Grundprinzipien fort.

Die DSGVO enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten (Art. 1 DSGVO).

Alle, die personenbezogene Daten in ihren Systemen verarbeiten, werden mit der DSGVO vor erhebliche technische und organisatorische Herausforderungen gestellt. Gerade im Bereich der Dokumentation und Nachweisbarkeit steigen die Anforderungen durch die Datenschutz-Grundverordnung erheblich. Es bietet sich an, entsprechende Datenschutz-Managementsysteme einzurichten.

Die wichtigsten Fakten zur DSGVO

- 88 Seiten
- 99 Artikel
- offizieller Titel: “Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG”
- Der erste Entwurf wurde bereits 2011 fertiggestellt.
- Die DSGVO gilt ab dem 25. Mai 2018 in der gesamten Europäischen Union.

Artikel 32 DSGVO – Datenschutz durch Technikgestaltung

In Artikel 32 DSGVO wird die Sicherheit der Datenverarbeitung geregelt. Dabei werden Maßnahmen und Schutzziele in Bezug auf die Prozesse, die verwendete Technik und Sicherheit der Datenverarbeitung aufgeführt. Diese beziehen sich sowohl unmittelbar auf die personenbezogenen Daten als auch auf die Systeme und Dienste, die im Zusammenhang mit der Datenverarbeitung eingesetzt werden (vgl. insbesondere Art. 32 Abs. 1 DSGVO).

.

Die Überprüfungs- und Aktualisierungspflicht erfordert, auch bestehende Verfahren regelmäßig zu überprüfen, insbesondere im Hinblick auf geänderte Rechts-vorschriften, auf wesentliche Verfahrungsänderungen , veränderte Zuständigkeiten sowie auf Weiterent-wicklungen hinsichtlich des Technikstandes.

Die 5 Gebote im Datenschutz

1. Verbot mit Erlaubnisvorbehalt
   Jede Datenverarbeitung, die nicht durch die Einwilligung des Betroffenen abgedeckt ist, bedarf der gesetzlichen Erlaubnis. Soweit kein Erlaubnistatbestand vorliegt, dürfen die Daten nicht verarbeitet werden.

2. Datensparsamkeit
   Eine Datenverarbeitung muss dem Zweck angemessen und sachlich relevant sowie auf das notwendige Maß beschränkt sein.

3. Zweckbindung
   Die Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben wurden. Im Fall einer Zweckerreichung sind die Daten zu löschen.

4. Datensicherheit
   Bei der Verarbeitung von Daten müssen geeignete technische und organisatorische Maßnahmen getroffen werden, um den Schutz vor Datenmissbrauch zu gewährleisten.

5. Transparenz
   Betroffene sollen wissen, dass und welche Daten in Bezug auf ihre Person erhoben wurden (u.a. Verfahrensverzeichnis, Löschkonzept etc.).

VIVA – Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität

Auch wenn in der DSGVO teilweise neue Begrifflichkeiten und Systematiken verwendet werden, finden sich doch letztendlich alle bisher schon aus den deutschen Datenschutzgesetzen abgeleitete Sicherheitsanforderungen auch in der Datenschutz-Grundverordnung wieder.

Das dabei geforderte **VIVA-Modell** – **V**ertraulichkeit, **I**ntegrität, **V**erfügbarkeit und **A**uthentizität der Datensicherheit – entspricht voll und ganz den Zielen der seit Jahren bei on-geo gelebten IT-Strategie.

V · I · V · A – Modell

- VERTRAULICHKEIT
  Schutz vor unbefugter Kenntnisnahme
- INTEGRITÄT
  Gewährleistung, Vollständigkeit, Zurechenbarkeit, Urheberschaft und (Rechts)Gültigkeit der Daten
- VERFÜGBARKEIT
  zeitgerechte Bereitstellung von Daten, Möglichkeit zur ordnungsgemäßen Verarbeitung
- AUTHENTIZITÄT
  Gewährleistung von den Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit

Mit der BaFin zielkonform beim Datenschutz

Die Forderung nach Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität sind ebenfalls in der MaRisk und in den BAIT zu finden. Die BaFin und somit letztendlich auch entsprechende Auftraggeber haben damit die identische Zielsetzung wie die on-geo GmbH. Eine diesen Anforderungen entsprechende IT-Strategie gibt es bei on-geo bereits seit 2016. Bei der strategischen Ausrichtung der IT beobachtet on-geo stetig die Relevanz von gesetzlichen und normativen Änderungen sowie technischen Weiterentwicklungen.

Vorgaben der Finanzaufsicht BaFin im Fokus

Die aufsichtsrechtlichen Anforderungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) bilden eine von zahlreichen datenschutzrechtlichen Grundlagen für die Geschäftstätigkeit und -entwicklung von on-geo. Die Einhaltung der aufsichtsrechtlichen Anforderungen ist dabei eine Selbstverständlichkeit. Jüngst wurde die MaRisk durch die BaFin novelliert und der Bereich Outsourcing weiter in den Fokus gerückt.

Um die Ziele der IT-Strategie von on-geo zu erreichen, wurden in den Prozessen einzelne Kontroll-punkte etabliert. Auf verschiedenen Ebenen finden regelmäßige sowie anlassbezogene Prüfungen statt, um die Wirksamkeit und Leistungs-fähigkeit der technischen und organisatorischen Maßnahmen zu messen.

Durch transparente Prozesse und regelmäßige Berichterstattung stellt on-geo sicher, dass die Auftraggeber die von der Aufsicht geforderten Kontroll- und Steuerungs-möglichkeiten erfüllen können.

Berichte aus dem internen Kontroll-System (IKS) und externe Überprüfungen bei der on-geo GmbH

- Jahresdatenschutzbericht
- Risiko- und Sichheitslagebericht
- Revisionsbericht
- SLA-Reports

DSGVO Compliance passende Lösungen

DSGVO – Anforderung	on-geo Lösung
Verfügbarkeit der Datensysteme	– Redundante IT-Systeme + – aktive Sicherheitsmaßnahmen + – Monitoring – on-geo eigenes hochqualifiziertes IT-Admin Personal + – Ständige Besetzung (24/7) der IT-Administration
Wiederherstellbarkeit der Daten – Notfallkonzepte für Rechenzentren, um nach einem Ausfall oder Angriff schnell wieder betriebsbereit zu sein	– regelmäßige Datensicherung mit Wiederherstellungstests – Notfallkonzepte
Privacy by design/Privacy by default Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung	– technische und organisatorische Maßnahmen für Hosting (Betrieb) und Verarbeitung – Security Features in LORA® wie Berechtigungskonzept – benötigte Menge personenbezogener Daten
Privacy by design/Privacy by default	**LORA® Sign** – ist eine fortgeschrittene elektronische Signatur nach Artikel 26 der EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen (eIDAS)

DSGVO Compliance passende Lösungen

DSGVO – Anforderung	on-geo Lösung
Privacy by design/Privacy by default	**LORA® Datenanonymisierung** – ermöglicht Daten zum Kunden und Eigentümer zu löschen bzw. zu anonymisieren – Ein Wiederherstellen der anonymisierten Daten in LORA ist nicht möglich.
Privacy by design/Privacy by default	**LORA® Mobile iPad Applikation** – datenschutzsichere Anmeldung – Löschung sämtlicher LORA® Mobile App-Daten auf dem Endgerät nach mehrmaliger Falscheingabe (5 Versuche) – nach Abschluss eines Besichtigungsauftrages erfolgt die umgehende physische Löschung der Daten – die iPad-Applikation verwendet zur Datenablage einen eigenen von den allgemeinen Daten getrennten Container
Privacy by design/Privacy by default	**LORA® Modul Datenschutz mitarbeiter-bezogener Daten** – ermöglicht die Ausblendung mitarbeiterbezogener Felder in den Sichten der Auftragsverwaltung – Dadurch werden solche Detailauswertungen nur für berechtigte Personen möglich.

DSGVO Compliance passende Lösungen

DSGVO - Anforderung	on-geo Lösung
Privacy by design/Privacy by default	**LORA® Modul Mitarbeitermandant (Organkredit) und LORA® Modul VIP-Mandant (VIP-Kredit)** – Gutachten sind nur durch berechtigte LORA® - Anwender des Instituts einsehbar und bearbeitbar
Meldefristen bei Datenpannen	abgestimmte Meldewege zwischen Auftraggebern und on-geo sichern eine fristgerechte Meldung im unwahrscheinlichen Falle einer Datenpanne
Rechte der Betroffenen	qualifizierte und zeitgerechte Unterstützung bei der Erfüllung gesetzlicher Verpflichtungen gegenüber der betroffenen Person

Über die on-geo GmbH

on-geo® gehört seit 2002 zu den führenden europäischen Anbietern von softwaregestützten Immobilienbewertungen. Und das aus gutem Grund, denn on-geo® liefert faktenbasierte Qualität. Als kompetenter Partner der Immobilien- und Finanzwirtschaft in allen Bewertungsfragen zählt on-geo unter anderem Finanzinstitute, Gutachter, Investoren, Finanzvermittler und Immobilienmakler zu seinen zufriedenen Kunden.

Datenschutz und Datensicherheit werden bei on-geo® groß geschrieben. Alle on-geo®-Mitarbeiter sind zur Verschwiegenheit nach § 5 BDSG und zur Wahrung des Bankgeheimnisses verpflichtet. Zur Sicherung der Datenübertragung finden Firewall, VPN, Virenschutz, SSL/TLS, Passwortschutz und Verschlüsselung Einsatz. Alle Auftraggeber haben dazu ein jederzeitiges Kontrollrecht. Alle datenverarbeitenden Systeme unterliegen bei on-geo® einem geregelten Datensicherungs-verfahren. Es werden zu verschiedenen Zeiten Backups durchgeführt und mehrere Generationen aufbewahrt. Kopien der Backups werden gesondert aufbewahrt.

on-geo®
Die Sicherheit, die Ihre Arbeit schützt