DSGVO

Technik und Sicherheit der Datenverarbeitung

Stand: 30.05.2020
Klaus Rathsfeld
Datenschutz- und Informationssicherheitsbeauftragter der on-geo GmbH

Inhaltsübersicht

Die Datenschutz-Grundverordnung (DSGVO)

Am 25. Mai 2018 trat die europaweit gültige Datenschutz-Grundverordnung in Kraft und ersetzte speziell in Deutschland das bisher gültige Bundesdatenschutzgesetz (BDSG_alt).

Aus diesem Grund haben wir gemeinsam mit unserem internen Datenschutz- und Sicherheitsbeauftragten ein E-Book entwickelt, welches Ihnen die zentralen Inhalte übersichtlich darstellt und aufzeigt, wie die on-geo GmbH mit den strengen Anforderungen umgeht.

Was ist die Datenschutz-Grundverordnung?

Die DSGVO stellt die Rechte und Freiheiten der betroffenen Personen – also derjenigen, deren personenbezogene Daten verarbeitet werden – in den Vordergrund und schreibt dabei 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 Unternehmen, 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-Grund-verordnung erheblich. Es bietet sich an, entsprechende Datenschutz-Managementsysteme einzurichten.

Fakten zur DSGVO

- Umfang: 88 Seiten und 99 Artikel

- Der offizielle Titel lautet:

“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 im Jahr 2011 fertiggestellt

- Die DSGVO gilt seit dem 25. Mai 2018

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 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.).

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

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 – Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Datensicherheit – entspricht voll und ganz den Zielen der seit Jahren bei on-geo gelebten IT-Strategie.

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.

Um die Ziele der IT-Strategie von on-geo zu erreichen, wurden in den Prozessen einzelne Kontrollpunkte etabliert. Auf verschiedenen Ebenen finden regelmäßige sowie anlassbezogene Prüfungen statt, um die Wirksamkeit und Leistungsfähigkeit 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 Steuerungsmöglichkeiten erfüllen können.

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.

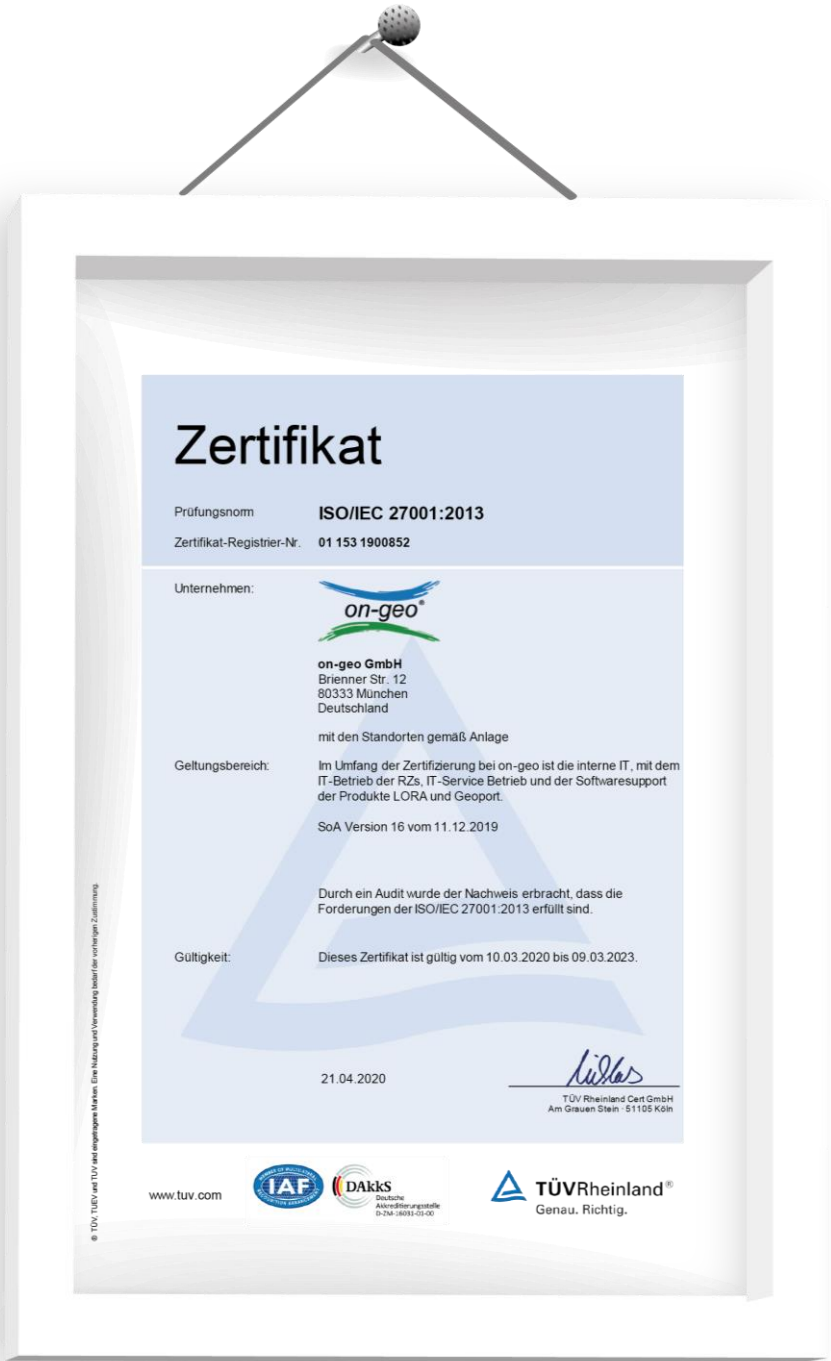
Berichte aus dem internen Kontroll-System (IKS) und externe Überprüfungen bei der on-geo GmbH

- Jahresdatenschutzbericht
- Risiko- und Sichheitslagebericht
- Revisionsbericht
- Zertifikate Rechenzentrum
- Zertifikate on-geo GmbH
- SLA-Reports

Informationssicherheits-Management

Die on-geo GmbH hat für ihr Informationssicherheits-Management von dem TÜV Rheinland die **Zertifizierung** nach dem **international anerkannten Sicherheitsstandard ISO 27001** erhalten.

Im Rahmen des Audits wurden alle sicherheitsrelevanten IT- und Geschäftsprozesse von on-geo umfassend geprüft und zertifiziert.



Zertifikat

Prüfungsnorm ISO/IEC 27001:2013

Zertifikat-Registrier-Nr. 01 153 1900852

Unternehmen:

on-geo GmbH
Brienner Str. 12
80333 München
Deutschland

mit den Standorten gemäß Anlage

Geltungsbereich: Im Umfang der Zertifizierung bei on-geo ist die interne IT, mit dem IT-Betrieb der RZs, IT-Service Betrieb und der Softwaresupport der Produkte LORA und Geoport.

SoA Version 16 vom 11.12.2019

Durch ein Audit wurde der Nachweis erbracht, dass die Forderungen der ISO/IEC 27001:2013 erfüllt sind.

Gültigkeit: Dieses Zertifikat ist gültig vom 10.03.2020 bis 09.03.2023.

21.04.2020

TÜV Rheinland Cert GmbH
Am Grauen Stein · 51105 Köln

www.tuv.com

TÜVRheinland®
Genau. Richtig.

Das Zertifikat belegt das Vorhandensein und die Wirksamkeit des Risikomanagement-Systems sowie des Informationssicherheitsmanagement-Systems in unserem Unternehmen.

Die ISO 27001 ist ein international anerkannter Beleg um ausreichend Garantien für die Einhaltung des Datenschutzes zu gewährleisten.

on-geo Lösungen – DSGVO compliant

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)
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

on-geo Lösungen – DSGVO compliant

DSGVO – Anforderung	on-geo Lösung
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 Besichtigungs-auftrages 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 Ansichten der Auftragsverwaltung • Detailauswertungen somit nur für berechtigte Personen möglich.
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

Die on-geo GmbH ist ein PropTech-Unternehmen mit Sitz in Erfurt. Das Unternehmen wurde 2002 von Dr. Klaus Wiegel gegründet. Heute ist die on-geo GmbH mit der LORA® Immobilienbewertungslösung, dem geoport Webshop und seinem Expertennetzwerk für die Besichtigung und die Wertermittlung von Immobilien Marktführer in Deutschland. Von den Standorten München, Erfurt und Wien aus agiert die on-geo GmbH mit derzeit 160 Mitarbeitern mittlerweile europaweit.

95 Prozent aller Sparkassen und Banken in Deutschland nutzen LORA als Standardlösung für die Immobilienbewertung. Es werden jährlich mehr als 1,5 Millionen Immobilien-Wertgutachten mit der webbasierte Bewertungssoftware erstellt. Über geoport werden monatlich mehr als 160.000 Markt- und Geodaten abgerufen.

Weitere Infos unter www.on-geo.de

Wir sind Ihr verlässlicher Partner für sicheres und rechtskonformes Arbeiten

on-geo GmbH
Parsevalstraße 2
99092 Erfurt

Telefon: 0800 6643677
Fax: 089 444 508 04

kontakt@on-geo.de
www.on-geo.de