LAUX
LAWYERS AG
ZURICH | BASEL

GDPR-Readiness

Projektleitfaden zur Umsetzung
der GDPR für Unternehmen

SIND SIE GDPR-READY?

Die neue EU Datenschutz-Grundverordnung (englisch „General Data Protection Regulation“ oder kurz „GDPR“) gilt ab dem 25. Mai 2018. Ab diesem Zeitpunkt hat die Verarbeitung von Personendaten im Anwendungsbereich der GDPR nach den neuen Vorschriften zu erfolgen. Auch viele Schweizer Unternehmen werden davon direkt betroffen sein.

Doch was heisst dies nun konkret für ein Unternehmen, das betroffen sein könnte?

Ein Unternehmen sollte sich die folgenden Fragen stellen:

- **Wo in meinem Unternehmen werden Daten verarbeitet?**
- **Welche Verarbeitungsprozesse umfassen Personendaten im Sinne der GDPR?**
- **Welches sind die geeigneten technischen und organisatorischen Massnahmen für die konkreten Verarbeitungen in meinem Unternehmen?**
- **Wie verarbeite ich Personendaten „rechtmässig“ im Sinne der GDPR?**
- **Und wo beginne ich überhaupt mit der Analyse und Umsetzung?**

Ohne ein systematisches Herangehen lassen sich diese Fragen nicht beantworten. Unternehmen sollten die richtigen Arbeiten an die Hand nehmen – zielgerichtet und organisiert, aber ohne in Aktivismus zu verfallen. Oder Sie ziehen einfach den richtigen Partner für das GDPR-Umsetzungsprojekt bei. Einen Partner wie LAUX LAWYERS AG.

Dieser Projektleitfaden beschreibt die Arbeiten, die im Rahmen eines GDPR-Umsetzungsprojekts vorgenommen werden sollten. Nicht alle sind schon vor dem 25. Mai 2018 zu erledigen. Nicht alle davon müssen zwingend umgesetzt werden. Und vieles davon kann unternehmensintern mit fachkundiger Begleitung ausgeführt werden. Entscheidend ist, dass die Umsetzung der konkreten Situation und Gefährdungslage für personenbezogene Daten im Unternehmen gerecht wird, also angemessen ist.

Mit diesem Projekt-Leitfaden erhalten Sie einen Überblick, wie die Herausforderung GDPR in drei Phasen zu meistern ist:

PHASE 1

Zunächst ist es erforderlich, Erhebungen zum **IST-Zustand** vorzunehmen. Die GAP-Analyse zeigt auf, inwiefern der IST-Zustand der GDPR nicht genügt.

PHASE 2

Anschliessend wird der **SOLL-Zustand** festgelegt. Auf Basis der GAP-Analyse werden Umsetzungsmassnahmen getroffen.

PHASE 3

Der nach Abschluss des Projekts erreichte Zustand wird in Form eines **Abschlussberichts** dokumentiert, um intern sowie gegenüber Dritten die GDPR-Readiness nachweisen zu können.

Die Phasen 1 und 2 werden jeweils nach der bewährten PDCA-Methode durchgeführt:

PLAN
Planung des Vorgehens

DO
Umsetzungshandlungen

CHECK
GAP-Analyse oder Wirksamkeitsanalyse

ACT
Einführung in der Breite und regelmässige Überprüfung

PHASE 1
IST-Zustand

In Phase 1 geht es um die Sachverhaltserhebung sowie die GAP-Analyse im Sinne einer sicherheitstechnischen und datenschutzrechtlichen Lückenanalyse, d. h. die aus rechtlicher Warte erfolgende Bewertung, ob der IST-Zustand der GDPR bereits genügt.

PLAN

1 Kick-off

Festlegung von Zielsetzungen und Erwartungen; Zeitplanung; Einführung in initiale Erhebungsunterlagen von LAUX LAWYERS AG.
Ziel: Verständnis über Ablauf des Projekts.

2 Individualisierung Erhebungsunterlagen

Individualisierung der Erhebungsunterlagen auf Verhältnisse beim Unternehmen.
Ziel: Vollständige Arbeitsunterlagen zur Erhebung des IST-Zustands.

DO

3 Erhebung IST-Zustand: Systeme, Applikationen und Daten

Erarbeitung Gesamtüberblick über System-, Applikations- und Datenlandschaft; Identifizierung von Risikobereichen; Erhebung erfolgt selbständig durch das Unternehmen auf Basis der zur Verfügung gestellten Unterlagen oder durch beigezogene Netzwerkpartner von LAUX LAWYERS AG.
Ziel: Vollständige Dokumentation der Systeme, Applikationen und Daten.

4 Erhebung IST-Zustand: Prozesse, technische & organisatorische Massnahmen

Erarbeitung Gesamtüberblick über technische & organisatorische Massnahmen; Identifizierung von Risikobereichen; Erhebung erfolgt selbständig durch das Unternehmen oder durch beigezogene Netzwerkpartner von LAUX LAWYERS AG.
Ziel: Vollständige Dokumentation der technischen & organisatorischen Massnahmen und Prozesse.

5 Erhebung IST-Zustand: Verträge

Analyse der bestehenden Verträge mit Lieferanten (Inbound) und mit Kunden (Outbound); Übersicht über internationale Datenaustausche.
Ziel: Identifikation von Handlungsbedarf und Aufzeigen von Bereinigungsoptionen.

6 Erhebung IST-Zustand: Weisungswesen, Compliance

Inventarisierung und Due Diligence der vorhandenen Weisungen und Compliance-Prozesse.
Ziel: Bewusstsein über Organisation bzgl. Datenverarbeitungen.

CHECK

7 Bereinigung und Vollständigkeitsanalyse IST-Zustand

Finalisierung der Dokumentationen zum IST-Zustand.
Ziel: Bereinigte und vollständige Dokumentation zum IST-Zustand.

8 GAP-Analyse

Bewertung des IST-Zustands (GAP-Analyse) in Berichtform.
Ziel: Unternehmen versteht, inwiefern der IST-Zustand der GDPR nicht genügt.

ACT

Aufbauend auf den Erkenntnissen aus Phase 1 werden in Phase 2 die erforderlichen Massnahmen festgelegt und umgesetzt.

PHASE 2
SOLL-Zustand

PLAN

9 Definition SOLL-Zustand

Planung des SOLL-Zustands auf Grundlage der GAP-Analyse.
Ziel: Anforderungen an SOLL-Zustand sind definiert.

10 Planung Umsetzungsmassnahmen

Definition von Massnahmen zur Erreichung des SOLL-Zustands; Aufbereitung von Handlungsempfehlungen; Roadmap zur Erreichung eines abgesicherten Compliance-Levels.
Ziel: Massnahmen zur Erreichung des SOLL-Zustands sind definiert.

11 Datenschutz-Folgenabschätzung: Evaluation Notwendigkeit

Rechtliche Beurteilung, ob Datenschutz-Folgenabschätzungen bei gewissen Datenverarbeitungen notwendig oder sinnvoll ist.
Ziel: Entscheidungsgrundlagen zur Notwendigkeit von Datenschutz-Folgenabschätzungen.

DO

12 Umsetzung Empfehlungen zum SOLL-Zustand

Technische Beratung; Organisationsentwicklung; Prozessentwicklung und -optimierung für Datenerhebungen und -bearbeitungen; Anpassungen in Verträgen (Inbound, Outbound); Unterstützung in der Umsetzung oder direkte Umsetzung durch LAUX LAWYERS AG oder Netzwerkpartner.
Ziel: Unternehmen hat empfohlene Massnahmen umgesetzt.

13 GDPR in IT-Governance

Implementierung GDPR in IT-Governance-Vorgaben, Datenschutz-Richtlinien, Prozess-Leitfäden etc.
Ziel: Sicherstellung Integration GDPR-Vorgaben.

14 Erstellen datenschutzbezogenes Weisungswesen

Erstellen von Weisungen zur Stützung der internen Abläufe und zur Stärkung der Compliance-Landschaft im Unternehmen.
Ziel: Datenschutzkonformes Weisungswesen etabliert.

15 Datenschutz-Folgenabschätzung: Durchführung

Durchführung Datenschutz-Folgenabschätzung bei bestehenden Systemen; Analyse, Bewertung, Dokumentation, Vornahme von Meldungen; Schlussbericht.
Ziel: Vorgaben GDPR betr. Datenschutz-Folgenabschätzungen sind erfüllt.

16 Schulung Mitarbeiter

Zweitägiger Kurs, welcher Mitarbeitern einen Überblick über Rechte und Pflichten im Zusammenhang mit der Verarbeitung von personenbezogenen Daten gibt;
3 Module: (i) Fundamentals Privacy; (ii) Organisation; (iii) Privacy in der Praxis.
Ziel: Unternehmen sorgt für Grundwissen und Awareness bei Mitarbeitern.

17 Erstellen von Checklisten und Arbeitshilfen

Checklisten und Arbeitshilfen für datenschutzrelevante Tätigkeiten im Unternehmen.
Ziel: Unternehmen erhält praktische Hilfestellung zum eigenen situativen Einsatz.

CHECK

18 Umsetzungskontrolle aus rechtlicher Sicht

Rechtliche Beurteilung der umgesetzten Massnahmen. Nennung der noch nicht erfolgreich umgesetzten Positionen.
Ziel: Erkenntnis nach innen: Unternehmen weiss, ob die umgesetzten Massnahmen erfolgreich waren und den SOLL-Zustand abbilden.

19 Wirksamkeitsprüfung

Beurteilung der vom Unternehmen umgesetzten Massnahmen in Bezug auf deren Wirksamkeit; mittels Stichproben wird festgestellt, ob die umgesetzten Massnahmen die erwünschten Wirkungen zeigen.
Ziel: Erkenntnis nach innen: Unternehmen weiss, ob tatsächlicher Schutz sich verbessert hat.

ACT

20 Etablierung datenschutzbeauftragte Person

Recruiting: Interne datenschutzbeauftragte Person (im Anstellungsverhältnis)

Definition Aufgabenbeschreibung bzw. Stellenbeschreibung; Scouting und Unterstützung bei der Auswahl; Einweisung.
Ziel: Das Unternehmen hat eine datenschutzbeauftragte Person bestellt.

Service: Externe datenschutzbeauftragte Person (DSB as a Service)

Ausführung der Aufgaben der datenschutzbeauftragten Person durch LAUX LAWYERS AG gemäss Aufgabenbeschreibung.
Ziel: Unternehmen hat eine datenschutzbeauftragte Person im Einsatz.

21 Laufende datenschutzrechtliche Beratung

Klärung von täglichen oder aussergewöhnlichen Problemstellungen; Wahrung von Betroffenenrechten, Arbeit bzw. Austausch mit Behörden etc.; Unterstützung der bestellten datenschutzbeauftragten Person bei Bedarf; datenschutzrechtliches Housekeeping im Allgemeinen.
Ziel: Aufrechterhalten der Datenschutz-Compliance auf Dauer.

PHASE 3
DOKUMENTATION

22 Abschlussbericht

Im Rahmen eines Abschlussberichts wird managementgerecht dargestellt, welche Tätigkeiten zur Umsetzung der „Herausforderung GDPR" vorgenommen wurden und welchen Stand das Unternehmen als Folge davon erreicht hat.
Ziel: Unternehmen verfügt über Dokumentation der Arbeiten, die dem Management gegenüber die Resultate darstellt.

23 Ergänzende Compliance-Dokumentationen (nach Bedarf)

Rechtsgutachten und/oder Audit-Bericht, die bei Bedarf Dritten oder Behörden vorgewiesen werden können, um Compliance mit der GDPR nachzuweisen.
Ziel: Dokumentation nach aussen. Unternehmen kann seine Massnahmen dokumentiert vorweisen.

24 Begleitendes Arbeitspaket „Vorhabenskoordination"

Koordination sämtlicher Aspekte und Erwartungen an das Projekt, insb.: Steuerung Projektdauer und Termine, Kosten bzw. Aufwände sowie Inhalt, Umfang und Qualität der vereinbarten Ergebnisse.
Ziel: Gesamtkoordination des Projekts.

ÜBER UNS

LAUX LAWYERS AG führt im Verbund mit internationalen Partnern europaweit Prüfungen zur GDPR-Compliance durch. Wir beraten Sie gerne oder begleiten Ihr Unternehmen durch den gesamten Prozess – von der Planung bis zur Abschluss-dokumentation. Dies in Zusammenarbeit mit bewährten Netzwerkpartnern (insb. Informationssicherheitsexperten, Business Consultants etc.) und stets in engem Zusammenwirken mit Ihnen und unter optimaler Ausschöpfung interner Ressourcen.

Bitte kontaktieren Sie uns, wenn Sie mehr über die Leistungen von LAUX LAWYERS AG erfahren möchten. Gerne beantworten wir Ihre Fragen und definieren gemeinsam das weitere Vorgehen. Und stellen sicher, dass Sie rechtzeitig GDPR-Ready sind.

Ihre Ansprechpartner:

Alexander Hofmann
Rechtsanwalt lic. iur. (Zurich University) PGCert Computer & Communications Law (Queen Mary University, London)
alexander.hofmann@lauxlawyers.ch
T +41 44 880 24 24

Mark Schieweck
Rechtsanwalt lic.iur. (Basel University)
mark.schieweck@lauxlawyers.ch
T +41 61 283 06 06

BÜRO ZÜRICH
A Seegartenstrasse 2
P. O. Box 360 · CH 8024 Zürich
T +41 44 880 2424
F +41 44 880 2425
W www.lauxlawyers.ch

BÜRO BASEL
A Steinenring 40 · CH 4051 Basel
T +41 61 283 0606
W www.lauxlawyers.ch

RECHTSANWÄLTE
Z Dr. Christian Laux · LLM
Z Dr. Jürg Hess · MBA · M.C.J.
Z Alexander Hofmann
B Mark Schieweck

In den zuständigen
Anwaltsregistern eingetragen

Lawyers by Profession | IT Enthusiasts by Passion
Consultants by Curiosity | Partners by Conviction