

# So erstellen Sie ein erfolgreiches Datenschutzprogramm



✓ Pridatect

# Inhalt

01	Einleitung	
02	Schritte zu einem erfolgreichen Datenschutzprogramm	
	a) Die Geschäftsaktivitäten des Unternehmens kennen.....	4
	b) Analyse bestehender Risiken.....	5
	c) Feststellung, ob die Bestellung eines Datenschutzbeauftragten verpflichtend ist.....	6
	d) Identifizierung der Unternehmen, die Dienstleistungen erbringen und Zugriff auf Daten haben.....	7
	e) Inkenntnissetzen der Betroffenen.....	8
	f) Gute Schulungen für Unternehmen und Mitarbeiter .....	9
03	Schlussfolgerung	

## 01. Einleitung

Der Schlüssel zu einem guten Datenschutzprogramm liegt in einer umsichtigen Vorgehensweise sowie in der Durchführung der nachfolgenden Schritte.

Wir dürfen jedoch nicht vergessen, dass Organisationen einem steten Wandel unterliegen. Der eigentliche Erfolg bei der Realisierung eines Datenschutzprogramms liegt in ihrer ständigen Beobachtung, um immer auf dem aktuellen Stand zu sein.

Wenn beispielsweise in einem Unternehmen eine Liste darüber existiert, welche Mitarbeiter Zugriff auf personenbezogene Daten haben, muss diese bei jedem Personalwechsel aktualisiert werden. Auf diese Weise können die Verantwortlichkeiten festgestellt werden, wenn es zu einer Datenschutzverletzung kommt. Es ist nicht ausreichend, das Datenschutzprogramm einmal pro Jahr zu aktualisieren; es sollte kontinuierlich überprüft und angepasst werden.



## 02. Schritte zu einem erfolgreichen Datenschutzprogramm

Daher sollten die nachfolgend beschriebenen Schritte regelmäßig durchgeführt werden.

### a) Die Geschäftsaktivitäten des Unternehmens kennen

**Zur Einführung eines Datenschutzprogramms** ist es wichtig, das Unternehmen, bei dem Sie das Compliance-Programm durchführen, genau zu kennen.

Sie müssen die Geschäftsaktivitäten des Unternehmens kennen, um zu wissen, wie personenbezogene Daten verarbeitet werden.



**Beispielsweise** werden in einem Krankenhaus nicht dieselben Daten wie in einer Eigentümergemeinschaft verarbeitet: In einem Krankenhaus wird eine große Datenmenge verarbeitet, darunter besonders schützenswerte Daten wie Gesundheitsdaten oder Daten Minderjähriger. Eine Eigentümergemeinschaft verarbeitet hingegen weniger personenbezogene Daten, die zudem nicht so sensibel sind.

**Nach der Identifizierung der Verarbeitungstätigkeiten** muss das in Artikel 30 DSGVO geforderte Verzeichnis erstellt werden. Dabei ist zu berücksichtigen, welche Aktivitäten das Unternehmen als Verantwortlicher, Mitverantwortlicher, Auftragsverarbeiter oder Unterauftragsverarbeiter durchführt.

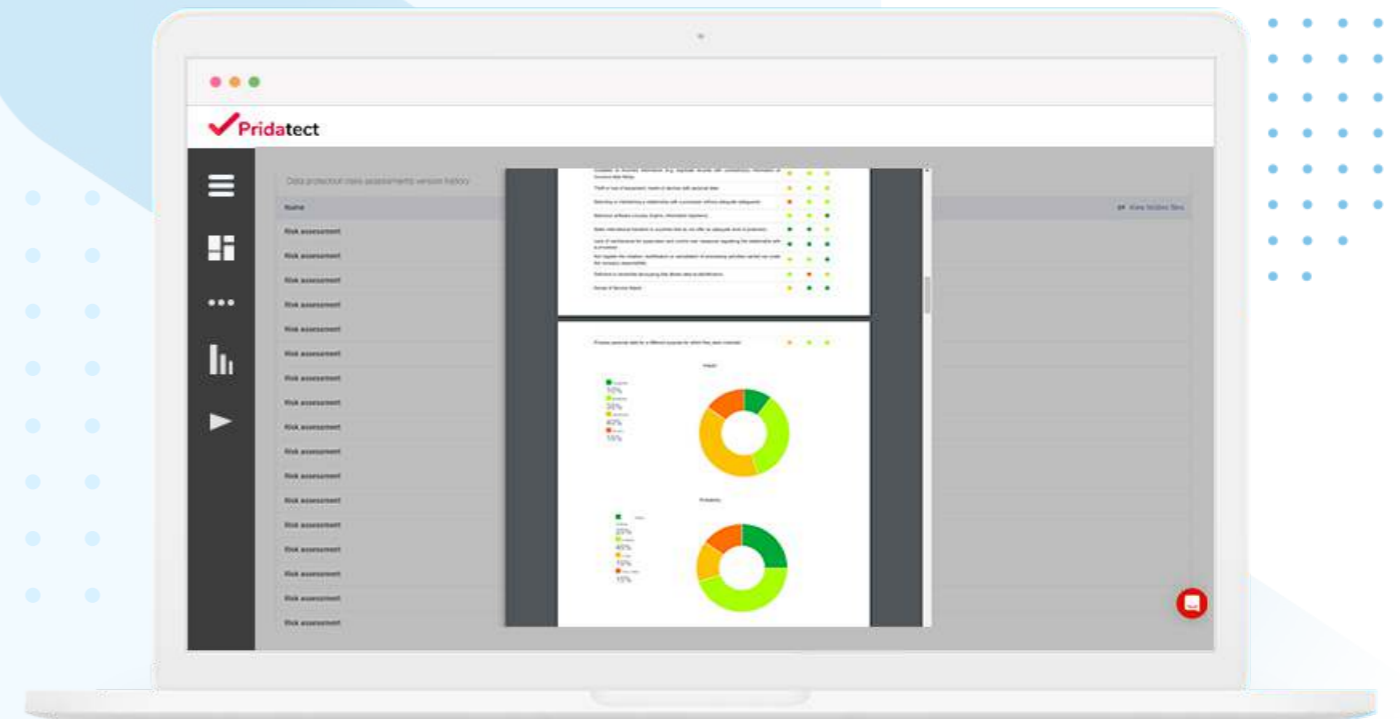
Die Erstellung dieses Verzeichnisses von Verarbeitungstätigkeiten ist die wesentliche Legitimationsgrundlage jeglicher Verarbeitung, ihrer Dauer, ihres Zwecks, internationaler Übermittlungen usw.

### b) Analyse bestehender Risiken

**Es muss analysiert werden**, welche Risiken die Verarbeitungstätigkeiten bergen, um für jedes Risikoszenario angemessene Schutzmaßnahmen festlegen zu können.

**Es ist sehr wichtig genau festzulegen**, welche Maßnahmen zu ergreifen sind, und zwar in Abhängigkeit von der Unternehmensgröße, des Technikstandards und der festgestellten Risiken. Die implementierten Maßnahmen müssen präventiv, eindämmend und korrigierend sein. Dabei muss zwischen technischen und organisatorischen Maßnahmen unterschieden werden.

**In einigen Fällen** müssen die Unternehmen eine Folgenabschätzung vornehmen. Durch eine vorgeschaltete Risikoanalyse können Sie feststellen, ob dies auch auf Ihr Unternehmen zutrifft.

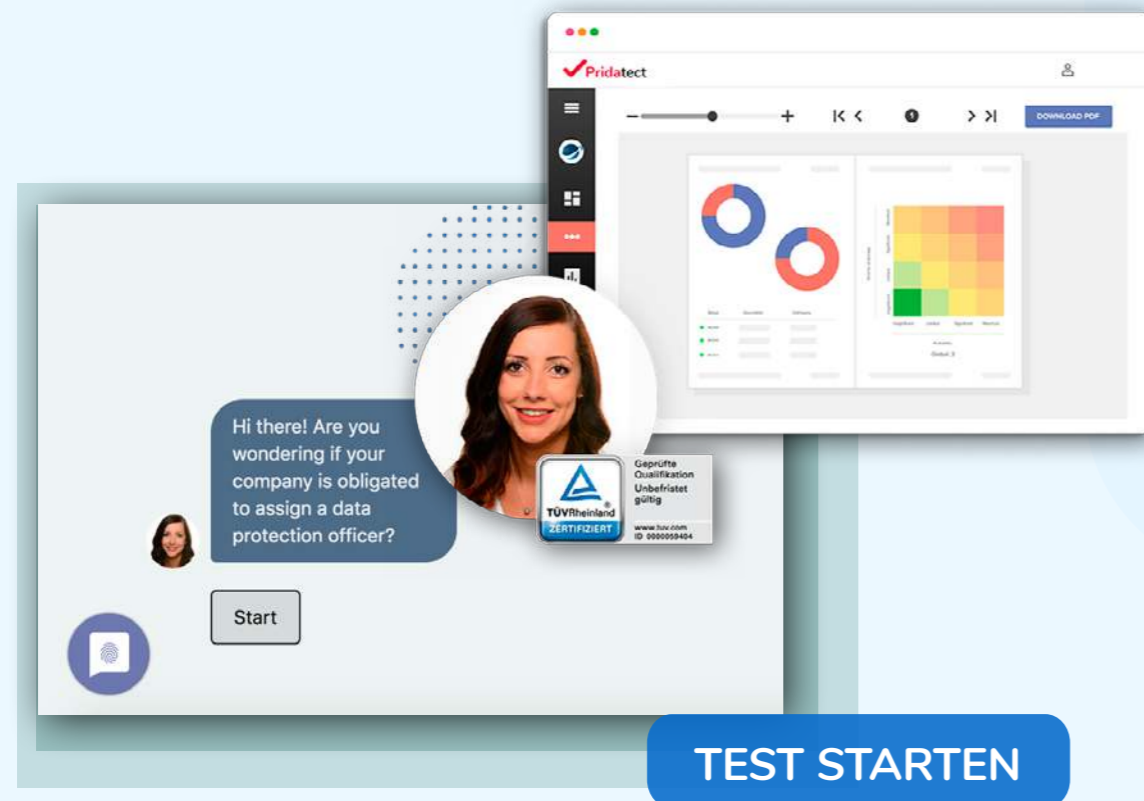


### c) Feststellung, ob die Bestellung eines Datenschutzbeauftragten verpflichtend ist

Artikel 37 der DSGVO schreibt die Bestellung eines Datenschutzbeauftragten in folgenden Fällen vor:

- **Wenn die Datenverarbeitung** von einer Behörde oder einer öffentlichen Stelle durchgeführt wird.
- **Wenn die Kerntätigkeit** der Organisation die regelmäßige und systematische Überwachung großer Gruppen Betroffener erforderlich macht.
- **Wenn zu den Kerntätigkeiten** der Organisation die umfassende Verarbeitung besonderer Kategorien personenbezogener Daten gehört.

Die Bestellung eines Datenschutzbeauftragten ist auch in den Fällen empfehlenswert, in denen sie nicht vorgeschrieben ist. Das Unternehmen kann von der Benennung profitieren, da hierdurch die Einhaltung der Vorschriften gewährleistet wird.



The image shows a desktop monitor displaying the Pridatetect web application. The interface includes a navigation menu on the left, a main content area with two donut charts and a heatmap, and a 'DOWNLOAD PDF' button. In the foreground, there is a circular profile picture of a woman, a 'Start' button, and a blue button labeled 'TEST STARTEN'. A speech bubble contains the text: 'Hi there! Are you wondering if your company is obligated to assign a data protection officer?'. A TUV Rheinland certification logo is also visible.

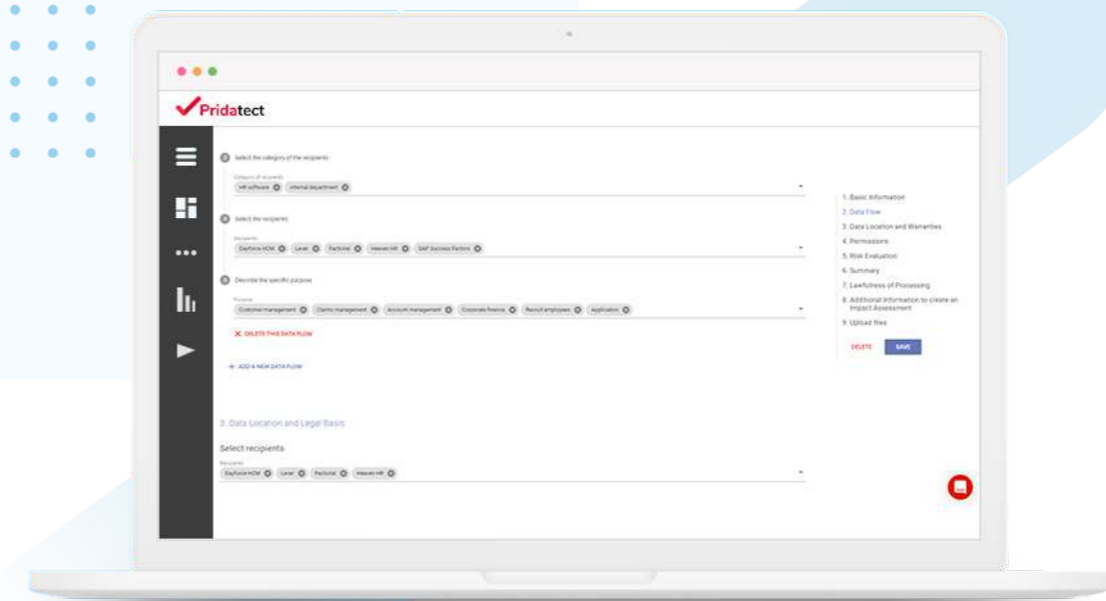
### d) Identifizierung der Unternehmen, die Dienstleistungen erbringen und Zugriff auf Daten haben

Ein weiterer sehr wichtiger Punkt bei der Sicherstellung des Datenschutzes ist die Identifizierung von Dienstleistungsunternehmen und -organisationen, die Zugriff auf Daten haben, um sie als Auftragsverarbeiter, Empfänger oder Zessionäre zu klassifizieren.

Die Identifizierung dieser Unternehmen dient auch der Feststellung, ob internationale Datenübermittlungen stattfinden und ob es die Garantien gibt, mit denen eine Datenübermittlung außerhalb der EU zulässig ist.

Es müssen Vereinbarungen oder Verträge über die Datenverarbeitung durch Dritte und über die Vertraulichkeit bei der Erbringung von Dienstleistungen geschlossen werden. Als unzulässig werden Auftragsverarbeiter angesehen, die solche Vereinbarungen nicht unterzeichnen oder die darin festgelegten

Maßnahmen nicht einhalten. Ohne die entsprechenden Garantien dürfen keine internationalen Datenübermittlungen erfolgen. Die Organisation muss daher bei der Auswahl von Lieferanten besonders umsichtig sein und die Zusammenarbeit beenden, wenn die Einhaltung nicht garantiert wird.

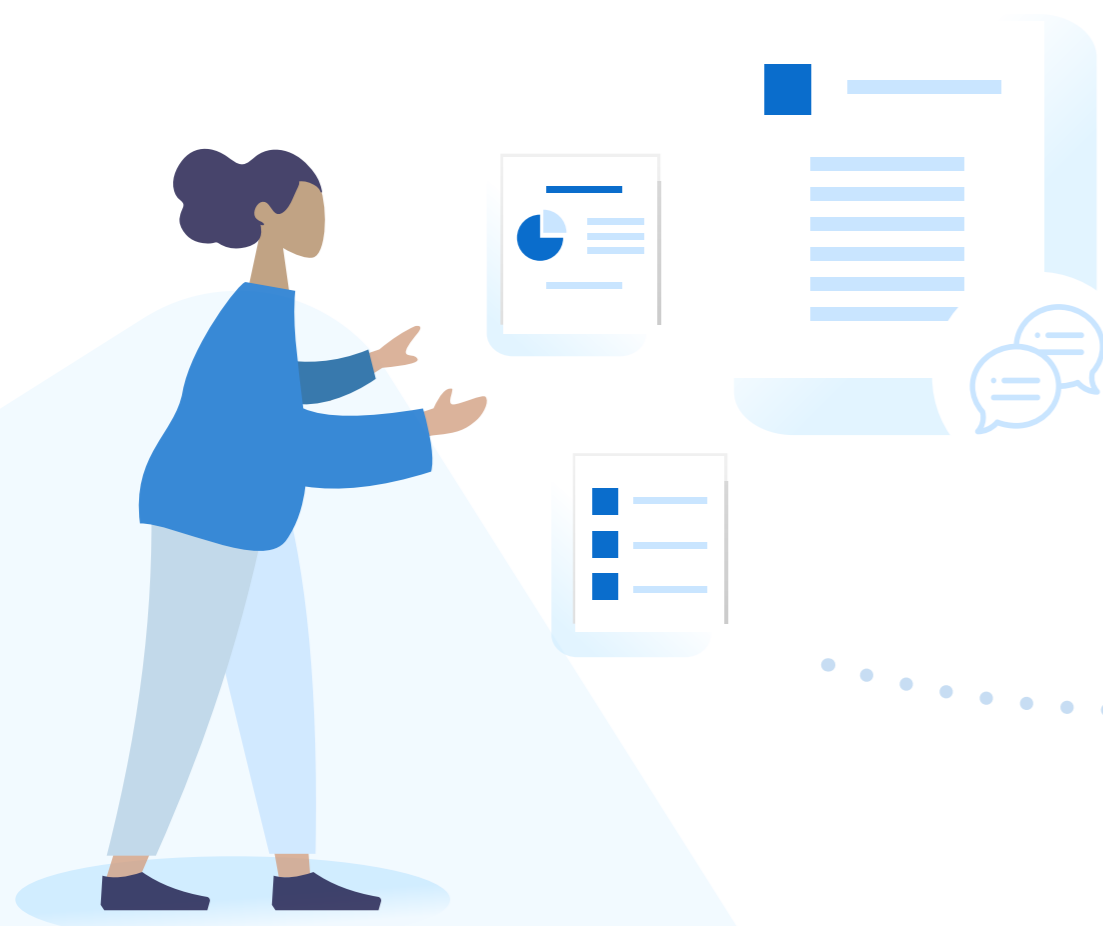


The image shows a laptop displaying the Pridatetect web application. The screen shows a form titled 'Select recipients' with a dropdown menu for 'Select recipients' and a 'SELECT THIS DATA FLOW' button. The right sidebar contains a list of steps: 1. Basic Information, 2. Data Flow, 3. Data Location and Warranties, 4. Permissions, 5. Risk Evaluation, 6. Summary, 7. Categories of Processing, 8. Additional Information to create an Impact Assessment, 9. Upload File. There are 'DELETE' and 'SAVE' buttons at the bottom right.

## e) Inkenntnissetzen der Betroffenen

Die wichtigste Verpflichtung des Regelwerks liegt in der Informationspflicht der Betroffenen darüber, dass ihre Daten verarbeitet werden. Diese Verpflichtung muss zum Zeitpunkt der Datenerfassung erfüllt sein.

Eine besondere Notwendigkeit zur Information der Betroffenen über die Datenerfassung besteht bei kommerzieller Kommunikation oder bei der Sammlung von Daten über das Internet. Eine gute praktische Vorgehensweise für ein erfolgreiches Datenschutzprogramm ist es, auf zwei Ebenen zu informieren: Auf der ersten Ebene werden grundlegende Informationen gegeben und ein Link mit zusätzlichen Informationen hinzugefügt. So erhält der Nutzer einen Überblick über die grundlegenden Informationen, selbst wenn er nicht auf die zweite Ebene zugreift.



## f) Gute Schulungen für Unternehmen und Mitarbeiter

Und schließlich ist einer der kritischen Punkte für die Einhaltung des Datenschutzes im Unternehmen oder in der Organisation die **Schulung aller beteiligten Personen**, damit sie wissen, wie sie mit den Daten umzugehen haben, wie sie bei Schutzverletzungen vorgehen und wie sie mit rechtlichen Anfragen umgehen müssen.

Dieser Punkt gibt den Ausschlag, ob die Organisation eine angemessene Compliance-Politik und -kultur hat.



## 03. Schlussfolgerung



**Ein gutes Datenschutzprogramm muss vollständig sein**, alle durch die Vorschriften auferlegten Pflichten abdecken und die Rechte natürlicher Personen gewährleisten. Dies geschieht mithilfe der aufgeführten Schritte, die regelmäßig wiederholt werden müssen.



**Obwohl die DSGVO keinen Zeitrahmen für Audits vorgibt**, ist es sehr vorteilhaft diese durchzuführen, um zu überprüfen, ob das Unternehmen die Vorschriften einhält und alle empfohlenen Maßnahmen umgesetzt hat.



**Wie auch sonst sind die Menschen der wichtigste Faktor für den Erfolg** eines Datenschutzprogramms. Daher ist es wichtig, jeden neuen Mitarbeiter zu schulen und von Zeit zu Zeit kleine Trainings durchzuführen. Es gilt zu bedenken, dass eine der häufigsten Ursachen für Schutzverletzungen menschliche Fehler sind und dass diese durch gute Schulungen vermieden oder verringert werden können.



**Eine gute Möglichkeit, ein Datenschutzprogramm umzusetzen**, besteht in der Nutzung einer Software wie Pridatetect, die alle wiederkehrenden Prozesse mit einem hohen Maß an Detailtreue erleichtert.

## Die Pridatetect-Plattform macht es einfach Risiken zu identifizieren und Daten zu schützen



### RISIKEN RECHTZEITIG ERKENNEN

Erkennen und identifizieren Sie Risiken bei der Verarbeitung personenbezogener Daten (Kunden, Mitarbeiter, Anbieter ...). Mit der Pridatetect-Plattform können wir Bedrohungen und Schwachstellen in Ihren Prozessen identifizieren und analysieren.



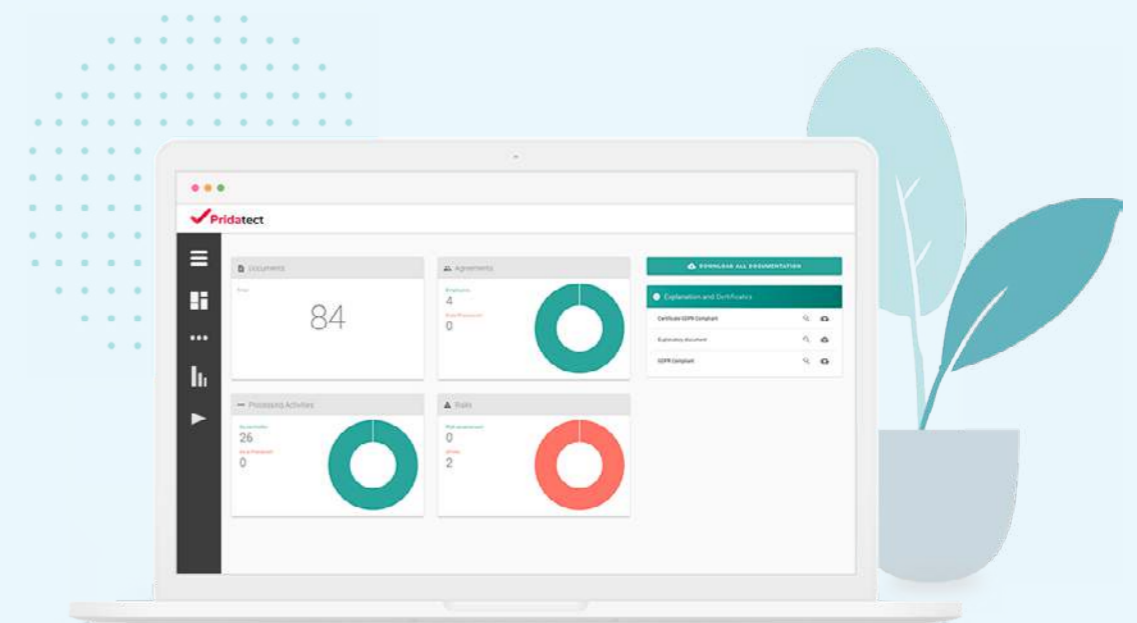
### MASSNAHMEN DEFINIEREN UND EMPFEHLEN

Nachdem wir die Risiken in Ihrem Unternehmen identifiziert haben, können wir erforderliche Maßnahmen definieren, um diese zu reduzieren. Pridatetect hilft schlägt notwendige Datenschutz-Maßnahmen für Ihr Unternehmen vor.



### ÜBERWACHUNG UND UMSETZUNG DES DATENSCHUTZES

Datenschutz ist eine ständige Aufgabe innerhalb eines Unternehmens. Pridatetect hilft nicht nur bei der ersten Implementierung, sondern auch bei der laufenden Überwachung und dem Aufgabenmanagement.



Kontaktieren Sie uns für eine [kostenlose Demo](#) oder nutzen Sie unsere [Testversion für 7 Tage gratis!](#)