# LEITFADEN
# PERSONEN-BEZOGENE DATEN

SAINT-GOBAIN

# INHALT

## **LEITFADEN**
## PERSONENBEZOGENE DATEN



REF-DE: 12/2017

# VORWORT

SAINT-GOBAIN

# VORWORT

**Die Verwendung von Informationstechnologie, Tablets, Smartphones, Apps, *Big Data* etc. macht aus Wirtschaftsakteuren Beteiligte einer digitalen Wirtschaft.**

**SAINT-GOBAIN durchläuft derzeitig einen digitalen Transformationsprozess, der Auswirkungen auf jede Aktivität innerhalb der Gruppe hat. Verstärkt wird dieser Prozess durch die massive Nutzung von Daten, die in immer größerer Menge, immer schneller und präziser gesammelt, verarbeitet und analysiert werden.**

**Es ist unsere Aufgabe, unter diesen Daten diejenigen zu erkennen, mit deren Hilfe eine natürliche Person in ihrem Arbeitsumfeld oder Privatleben unmittelbar oder mittelbar identifiziert werden kann.**

**Um diesen Praktiken einen Rahmen zu geben und die Risiken zu minimieren, hat die Europäische Union kürzlich eine Verordnung erlassen, die die Grundrechte und -freiheiten aller Bürger Europas unabhängig von ihrer Staatsangehörigkeit schützen soll.**

**Diese Datenschutz-Grundverordnung trat am 24. Mai 2016 in Kraft und wird ab dem 25. Mai 2018 in der gesamten EU gelten.**

In Übereinstimmung mit den Allgemeinen Verhaltens- und Handlungsprinzipien der Gruppe muss SAINT-GOBAIN diese neue Verordnung umsetzen.

Bleiben wir hier untätig, setzen wir uns unnötigen juristischen und operativen Risiken aus und schadet dem Ansehen der SAINT-GOBAIN Gruppe.

Mit den vorliegenden Merkblättern möchten wir Ihnen auf möglichst einfache Weise die Inhalte dieser neuen Verordnung vorstellen, damit Sie diese ab sofort umsetzen können.

Dieser Leitfaden bleibt dabei absichtlich recht allgemein. Beispiele illustrieren die unterschiedlichen Grundsätze und Regeln, die für die Verarbeitung personenbezogener Daten gelten, ohne jedoch all jene Fragen beantworten zu wollen. Bei konkreten Fragen wenden Sie sich bitte an Ihren Datenschutzbeauftragte oder Ihren Ansprechpa0rtner in der Rechtsabteilung.

Dieses Dokument soll alle SAINT-GOBAIN Mitarbeiter in Bezug auf die in der Verordnung definierten Begriffe, Rechte und Pflichten sensibilisieren und hat nicht den Anspruch, ein Rechtshandbuch zu sein.

Wir hoffen, dass dieses Dokument Ihnen einen hilfreichen Überblick gibt.

REF-DE: 12/2017

1

# UNTER WELCHEN BEDINGUNGEN GILT DIE VERORDNUNG?

SAINT-GOBAIN

# UNTER WELCHEN BEDINGUNGEN GILT DIE VERORDNUNG ?

1

## WORAUF IST SIE ANZUWENDEN?

Die Verordnung gilt für alle Daten, die es ermöglichen, eine natürliche Person direkt oder indirekt zu bestimmen (Name, SGID, aber auch IP-Adresse, Foto, Kennzeichen des Firmenwagens, Geo-Tracking-Daten etc.).

Unabhängig von der Art der Verarbeitung*: **Jedes Mal, wenn PD* gespeichert, weitergeleitet, übermittelt, eingesehen etc. werden.**

***PRAKTISCHES BEISPIEL***
Die Erstellung eines Firmenausweises für einen neuen Mitarbeiter mit Namen, Vornamen, SGID und Foto; Erstellung einer Kundenakte etc.

## WANN IST SIE ANZUWENDEN?

Wenn **der für die Verarbeitung Verantwortliche* in der EU* niedergelassen ist.**

***PRAKTISCHES BEISPIEL***
Ein Flachglas-Unternehmen mit Sitz in Deutschland verkauft online Waren nach Asien. Es erhebt Namen, Vornamen, Telefonnummern und Adressen der Empfänger, um die bestellten Waren liefern zu können.

Wenn der für die Verarbeitung Verantwortlich* außerhalb der EU* niedergelassen ist: **Wenn dort PD* einer natürlichen Person in der EU* verarbeitet werden** (siehe Diagramm unten auf der Seite).

***PRAKTISCHES BEISPIEL***
Ein Unternehmen der Aktivität Schleifmittel in den USA erhebt Namen, Vornamen und Telefonnummern von Kunden in der EU* für seine Kundendatenbank und um Informationen zu auf dem EU*-Markt verfügbaren Produkten schicken zu können.

ANWENDUNG DER VERORDNUNG

- **DER FÜR DIE VERARBEITUNG VERANTWORTLICHE* IST IN DER EU* NIEDERGELASSEN IST.** (Z.B. SAINT-GOBAIN)
- **WAREN UND DIENSTLEISTUNGEN WERDEN IN DER EU* ANGEBOTEN**
- **BEOBACHTUNG DES VERHALTENS DER BETROFFENEN PERSON* IN DER EU***

** siehe Merkblatt 15 „Definitionen"*



REF-DE: 12/2017

LEITFADEN PERSONENBEZOGENE DATEN


# RECHENSCHAFTSPFLICHT

SAINT-GOBAIN

# RECHENSCHAFTSPFLICHT

2

## WAS IST RECHENSCHAFTSPFLICHT?

*Jeder für die Verarbeitung Verantwortliche* muss in der Lage sein, die Einhaltung der Gesetzgebung* nachzuweisen.*
*Die Unternehmen werden stärker zur Verantwortung gezogen, insbesondere was das Management von Datenschutzrisiken betrifft.*

### IM GEGENZUG

Ab dem 25. Mai 2018 sind Unternehmen nicht mehr verpflichtet, Verarbeitungsvorgänge* von PD* an die Aufsichtsbehörde zu melden.

**Allerdings** ist für bestimmte Verarbeitungsvorgänge* ist die vorherige Genehmigung durch die zuständige Aufsichtsbehörde erforderlich (bestimmte Übermittlungen von PD*, Verarbeitungsvorgänge* mit einem hohen Risiko für Auswirkungen auf das Privatleben etc.).

## WELCHE PFLICHTEN GIBT ES?

Einführung eines Governance-Programms und einer Datenschutzrichtlinie*

Die Gruppe muss insbesondere ein Netzwerk von Datenschutzbeauftragten einrichten.

## IN DER PRAXIS

Der für die Verarbeitung Verantwortliche* muss folgende Maßnahmen umsetzen:

- Ernennung eines Datenschutzbeauftragten* (siehe Merkblatt 13)
- Führung eines Verzeichnisses aller Verarbeitungsvorgänge* (siehe Merkblatt 3)
- Einführung einer Datenschutzrichtlinie* sowie Erstellung von für Informationen, die für die alle Mitarbeiter und Partner verfügbar sind, insbesondere auf den Websites des Unternehmens
- Bewertung aller Verarbeitungsvorgänge* („Datenschutz durch Technik“ siehe Merkblatt 4, Datenschutzfolgenabschätzung siehe Merkblatt 5)
- Nachweis der Einhaltung der 5 Goldenen Regeln (siehe Merkblatt 14)
- Durchführung von Schulungen aller Mitarbeiter
- Einrichtung geeigneter Maßnahmen bei Übermittlung von PD* außerhalb der EU*
- Behebung und Meldung möglicher Datenschutzverletzungen (siehe Merkblatt 10)
- Durchführung von Überprüfungen der Regelkonformität in Bezug auf die Gesetzgebung*

** siehe Merkblatt 15 „Definitionen“*

REF-DE: 12/2017

LEITFADEN PERSONENBEZOGENE DATEN


# VERZEICHNIS VON VERARBEITUNGS-TÄTIGKEITEN, DATENZUORDNUNG

SAINT-GOBAIN

# VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN, DATENZUORDNUNG

3

## VERPFLICHTUNG ZUR FÜHRUNG EINES VERZEICHNISES

**Ab dem 25. Mai 2018** muss jedes SAINT-GOBAIN Unternehmen, **(i) das in der EU* niedergelassen ist oder (ii) das PD* von in der EU* wohnhaften Personen verarbeitet** (gemäß den Bedingungen in Merkblatt 1) **ein Verzeichnis führen**, dass alle Verarbeitungsvorgänge* von PD* umfasst.

### Ein Verzeichnis – zu welchem Zweck?

Um Verarbeitungsvorgänge von PD* **zu inventarisieren, zu überwachen und zu steuern.**

Jeder für die Verarbeitung Verantwortliche* muss eine ständig zu aktualisierendes Verzeichnis führen und im Falle einer Überprüfung nachweisen, dass es der Gesetzgebung* entspricht. *Siehe dazu auch Merkblatt 2 „Rechenschaftspflicht“*

## DATENZUORDNUNG (DATA MAPPING)

### Erforderlicher Schritt vor der Einrichtung eines Verzeichnisses

- Datenzuordnung bezeichnet die **Identifizierung** und **Nachverfolgung** von Verarbeitungsvorgängen* von PD* innerhalb eines Unternehmens
- Dies erfolgt per Audit oder Fragebogen durch die verschiedenen Personen, die PD* verarbeiten.

### ACHTUNG!

**Wenn ein Auftragsverarbeiter* eine Tätigkeit für einen Kunden durchführt, muss auch der Auftragsverarbeiter* ein Verzeichnis führen, dass diese Angaben enthält.**

**AB DEM 25. MAI 2018** WIRD SAINT-GOBAIN ÜBER EIN TOOL VERFÜGEN, DAS DIE ANFORDERUNGEN AN EIN VERZEICHNIS ERFÜLLT.

## INHALT DES VERZEICHNISSES: Was muss es genau beinhalten?

- **Angaben zum für die Verarbeitung Verantwortlichen*** sowie den Datenschutzbeauftragten bzw. die natürliche Person, die die Verarbeitung* durchführt.

  ***PRAKTISCHES BEISPIEL***
  Namen der Unternehmen, Namen und Kontaktdaten

- Den **Verarbeitungszweck***

  ***PRAKTISCHES BEISPIEL***
  Lohnbuchhaltung

- Eine **Beschreibung der Kategorien von betroffenen Personen*** sowie **von PD***

  ***PRAKTISCHES BEISPIEL***
  – Mitarbeiter, – Bankverbindung

- Die Kategorien von Empfängern der PD* (einschließlich der Empfänger außerhalb der EU*)

  ***PRAKTISCHES BEISPIEL***
  Buchhaltung (intern) und Banken (extern)

- Die Bezeichnung des Landes oder der internationalen Organisation bei Übermittlung von PD* außerhalb der EU* (siehe dazu auch Merkblatt 9 „Internationale Übermittlung von PD*“)
- Die Speicherdauer der PD*
- Das Verfahren zur Einholung der Einwilligung
- Eine allgemeine Beschreibung der **Datenschutzmaßnahmen,** insbesondere:
  - die Pseudonymisierung* und Verschlüsselung (Anonymisierung) der PD*
  - die operative Wartung der Verarbeitungssysteme
  - die Mittel zur Wiederherstellung der PD* nach einem Zwischenfall
  - die Verfahren, die regelmäßig für die Überprüfung, Analyse und Abschätzung der Wirksamkeit der Maßnahmen zur Verarbeitungssicherheit eingesetzt werden

** siehe Merkblatt 15 „Definitionen“*



REF-DE: 12/2017

LEITFADEN PERSONENBEZOGENE DATEN


# DATENSCHUTZ DURCH TECHNIK

SAINT-GOBAIN

# DATENSCHUTZ DURCH TECHNIK

4

## WAS BEDEUTET „DATENSCHUTZ DURCH TECHNIK“?

- Das Risiko von Datenschutzverletzungen sinkt, **wenn bereits vor dem Projekt die richtigen Schritte ergriffen werden.**
- **Der Schutz der PD* muss direkt in das Projekt *integriert werden*:** über die gesamte Laufzeit des Projekts hinweg, von der Schaffung des Projekts bis zu seiner wirtschaftlichen Nutzung:

Ein einfaches Beispiel für **Datenschutz durch Technik wäre die Herstellung eines Tagesbuchs mit einem Schloss**, anstatt es in einer Schublade einzuschließen.

**IDEE :**
**„LIEBER VORBEUGEN ALS REAGIEREN.“**

## KONKRETE MASSNAHMEN FÜR TECHNISCHEN DATENSCHUTZ

**PRIVACY BY DESIGN**

| | | |
|---|---|---|
| **Datenschutz** durch datenschutzfreundliche Voreinstellungen | Jedes Unternehmen, das PD* verarbeitet, muss standardmäßig für den höchstmöglichen Datenschutz sorgen. **Minimierung** der Datenerhebung auf jene Daten, die für den gewünschten Zweck absolut erforderlich sind. | *EXEMPLE* Auf einem Smartphone sind bei der Erstnutzung eines Programms die Optionen standardmäßig nicht aktiviert: Geo-Tracking, Zugriff auf Fotos etc. Die Aktivierung wird nach und nach vorgeschlagen. |
| **Speicherzeitraum und Löschung** von PD* | **Grundsatz: Der Zeitraum für die Speicherung von Daten** wird auf die Zeit begrenzt, die für den Verarbeitungszweck tatsächlich erforderlich ist. **Löschung** der Daten am Ende des Zeitraums | *EXEMPLE* PD* in Bezug auf Kunden oder potentielle Kunden dürfen bis zu drei Jahre nach dem letzten Kontakt mit dem (potentiellen) Kunden gespeichert werden. |
| **Sicherheitsmaßnahmen** je nach Risiko | Abhängig von der **Wahrscheinlichkeit**, der **Schwere** und dem **Ausmaß** der Verletzung der Rechte einer Person, z.B.<br>– **Pseudonymisierung***: So können Daten von der Bestimmung der betroffenen Person* getrennt werden. Sie kann naturgemäß **rückgängig gemacht werden**.<br>– **Anonymisierung**: Sie besteht darin, jegliche Möglichkeit der direkten oder indirekten Bestimmung der betroffenen Person* zu tilgen. Sie muss irreversibel sein.<br>– **Zugangssteuerung**<br><br>Einige Akteure wie z.B. Online-Banken haben obligatorische Sicherheitsmaßnahmen festgelegt. Für andere ist es erforderlich **Best-Practices zum Datenschutz** für die jeweilige Branche zu entwickeln. | *EXEMPLE* Standardmäßige SSL-Datenverschlüsselung beim Austausch sensibler Daten über das Internet. |

**DER RICHTIGE REFLEX:** DURCH DIE DOKUMENTIERUNG DER BEACHTUNG DES TECHNISCHEN DATENSCHUTZES IN PROJEKTE KÖNNEN IM FALLE EINER ÜBERPRÜFUNG DIE DATENSCHUTZBEMÜHUNGEN NACHGEWIESEN WERDEN. *(Siehe dazu auch Merkblätter 2 „Rechenschaftspflicht“ und 5 „Folgenabschätzung“)*

* *siehe Merkblatt 15 „Definitionen“*

REF-DE: 12/2017

LEITFADEN PERSONENBEZOGENE DATEN


# DATENSCHUTZ-FOLGEN-ABSCHÄTZUNG

SAINT-GOBAIN

# DATENSCHUTZFOLGEN-ABSCHÄTZUNG

5

## IN WELCHEN FÄLLEN IST EINE DATENSCHUTZ-FOLGENABSCHÄTZUNG ERFORDERLICH?

*Wenn eine Verarbeitungsart ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen* darstellen kann, muss der für die Verarbeitung Verantwortliche* vor der Durchführung des Verarbeitungsvorgangs eine Datenschutzfolgenabschätzung durchführen.*

Dies ist insbesondere erforderlich für die folgenden Verarbeitungsvorgänge von PD*:

- die systematische und eingehende Verhaltensüberwachung (z.B. Profilerstellung)
- die Massenverarbeitung besonderer Kategorien von PD* (z.B. biometrische Daten)

### WAS SIND BESONDERE KATEGORIEN VON PD*?

Das sind PD*, deren Verarbeitung* ein erhebliches Risiko für die Interessen der betroffenen Person* darstellen kann.

*PRAKTISCHES BEISPIEL:*
Angaben zur Rasse, Religion, ethnischen Herkunft, Gesundheitsdaten ...

## IN DER PRAXIS

- Ermitteln Sie, ob ein Risiko für die Rechte und Freiheiten der betroffenen Person* besteht und daher eine Datenschutzfolgenabschätzung erforderlich ist.
- Führen Sie eine Datenschutzfolgenabschätzung mit folgenden Inhalten durch:
  - eine Beschreibung des Verarbeitungsvorgangs* und seines Zwecks*
  - eine Abschätzung der Notwendigkeit und der Verhältnismäßigkeit des Verarbeitungsvorgangs*
  - eine Abschätzung der mit dem Verarbeitungsvorgang* verbundenen Risiken
  - die geplanten Maßnahmen

**Jede Landesaufsichtsbehörde wird eine nichterschöpfende Liste der Verarbeitungsvorgänge* veröffentlichen, bei denen eine Datenschutzfolgenabschätzung erforderlich ist.**

**DIE GRUPPE WIRD EINEN LEITFADEN VERÖFFENTLICHEN ZU:**

**– DER ERMITTLUNG DER ERFORDERLICHKEIT EINER DATENSCHUTZ-FOLGENABSCHÄTZUNG,**

**UND**

**– DER DURCHFÜHRUNG EINER DATENSCHUTZFOLGENAB-SCHÄTZUNG.**

**Kontaktieren Sie in diesen Fällen IHREN ZUSTÄNDIGEN DATENSCHUTZBEAUFTRAGTEN*.**

REF-DE: 12/2017

** siehe Merkblatt 15 „Definitionen"*

LEITFADEN PERSONENBEZOGENE DATEN


# EINWILLIGUNG DER BETROFFENEN PERSON

SAINT-GOBAIN

# EINWILLIGUNG DER BETROFFENEN PERSON

6

## HABE ICH DAS RECHT, PERSONENBEZOGENE DATEN* ZU VERARBEITEN?

**JA, ABER ...**
Ich muss mich an die **folgenden Vorgaben halten**:

### DIE HAUPTVERARBEITUNGSVORGÄNGE WURDEN GENEHMIGT.

- **Die betroffene Person* hat ihre Einwilligung erteilt.**

  *PRAKTISCHES BEISPIEL:*
  Abonnement eines Newsletters oder Teilnahme an einem Treuprogramm.

- **Der Verarbeitungsvorgang* ist notwendig für die Erfüllung des Vertrags.**

  *PRAKTISCHES BEISPIEL:*
  Kundenbestellung auf einer Online-Handelsseite.

- **Der Verarbeitungsvorgang* ist notwendig zur Erfüllung gesetzlicher Anforderungen.**

  *PRAKTISCHES BEISPIEL:*
  Pflichtmeldungen an die Finanzbehörden und Sozialversicherungsträger.

- **Der Verarbeitungsvorgang* ist durch ein rechtmäßiges Interesse des für die Verarbeitung Verantwortlichen* begründet.**

  *PRAKTISCHES BEISPIEL:*
  – Übermittlung von PD* an ein Kundendatenbank-Tool
  – Tool für die Lohnbuchhaltung

## WAS SIND DIE BEDINGUNGEN FÜR EINE RECHTLICHE GÜLTIGE EINWILLIGUNG ZUR VERARBEITUNG* VON PD*?

**Die Einwilligung muss folgende Bedingungen erfüllen:**

### OHNE ZWANG

Die Verarbeitung* von PD* darf nicht eine **Bedingung für eine Leistung** sein.

*PRAKTISCHES BEISPIEL:*
Die Erfüllung einer Bestellung darf nicht von der Erhebung unnötiger Angaben wie des Geburtsdatums abhängen.

### KONKRETER VERARBEITUNGSZWECK*

Die betroffene Person* erteilt ihre Einwilligung in die Nutzung ihrer PD* ausschließlich für einen **konkreten Zweck***.

*PRAKTISCHES BEISPIEL:*
Pflege der Geschäftsbeziehung

### KENNTNIS DER SACHLAGE

Die betroffene Person* muss **klare und einfach verständliche Information** erhalten.

### ACHTUNG

**ES MUSS MÖGLICH SEIN, DIE EINWILLIGUNG ZU JEDER ZEIT AUF EINFACHE WEISE ZU WIDERRUFEN.**

**ZUM BEISPIEL: „UNSUBSCRIBE"-LINK ZUR KÜNDIGUNG EINES NEWSLETTERS**

** siehe Merkblatt 15 „Definitionen"*



REF-DE: 12/2017

# EINWILLIGUNG DER BETROFFENEN PERSON

6

## WIE WIRD DIE EINWILLIGUNG DER BETROFFENEN PERSON* EINGEHOLT?

Die Einwilligung muss vor der Verarbeitung* der PD* **ausdrücklich erteilt werden (OPT IN*)**:

- Schriftlich oder (nachweisbar) mündlich
- Durch Anklicken eines Kästchens
- In einer App
- Durch ausdrückliches Verhalten

*PRAKTISCHES BEISPIEL:*
Abonnement eines Newsletters oder Teilnahme an einem Treueprogramm

## DARAUS FOLGT:

FOLGENDES STELLT KEINE EINWILLIGUNG DAR:

- **SCHWEIGEN**
- **VORAUS-GEFÜLLTE KÄSTCHEN**
- **ZUSTIMMUNG ZU VERKAUFS-/ NUTZUNGSBE-DINGUNGEN**

## → UND DAS OPT-OUT-MODELL*?

**DIES IST NUR IN SEHR WENIGEN FÄLLEN AUSREICHEND.**

## DER RICHTIGE REFLEX

- **Aufzeichnung mündlicher Einwilligungen (in Call-Centers etc.)**
- **Ankreuzkästchen**

*PRAKTISCHES BEISPIEL:*
„Ich bin damit einverstanden, Werbeanrufe im Namen der SG-Unternehmen zu erhalten."

## ACHTUNG:

**DER FÜR DIE VERARBEITUNG VERANTWORTLICHE* MUSS NACHWEISEN KÖNNEN, DASS ER VON DER BETROFFENEN PERSON* EINE WIRKSAME EINWILLIGUNG ERHALTEN HAT**
*(SIEHE MERKBLATT 2 „RECHENSCHAFTSPFLICHT").*

* *siehe Merkblatt 15 „Definitionen"*



REF-DE: 12/2017


# WELCHE RECHTE HABEN DIE BETROFFENEN PERSONEN?

SAINT-GOBAIN

# WELCHE RECHTE HABEN DIE BETROFFENEN PERSONEN?

7

## AUSKUNFTSRECHT

**Die betroffene Person*** hat das Recht, von dem für die **Verarbeitung Verantwortlichen*** folgende Angaben zu erhalten:

- **Informationen** zu seinen **Rechten**
- **Bestätigung** über die Verarbeitung der PD*
- **Zweck*** der **Verarbeitung***
- die **verarbeitete Kategorie** von **PD***
- **Empfänger** der PD*
- **Speicherdauer** der PD*
- **Quelle** der PD*, falls diese nicht direkt bei der betroffenen Person erhoben wurden
- Eventuell Nutzung eines **automatisierten Entscheidungssystem**

*PRAKTISCHES BEISPIEL:*
Die Verwendung eines automatisierten Systems zur Bewertung der Kreditwürdigkeit, um Kreditanfragen von Kunden ohne Einwirkung eines Menschen zu filtern

## WO BEFINDEN SICH DIESE INFORMATIONEN?

DIE INFORMATIONEN SIND IM VERZEICHNIS *(siehe Merkblatt 3)* ENTHALTEN.

## RECHT AUF EINSCHRÄNKUNG DER VERARBEITUNG*

**Die betroffene Person* kann verlangen, die Verarbeitung von ihren PD* zu unterbrechen,** um die Rechtmäßigkeit des Verarbeitungsvorgangs*, die Richtigkeit der Informationen oder die Notwendigkeit zur Speicherung von PD* zu überprüfen.

## RECHT AUF BERICHTIGUNG

Die betroffene Person hat das Recht auf **Berichtigung bzw. Vervollständigung** ihrer PD*.

## WIDERSPRUCHSRECHT

Die betroffene Person kann der **Verarbeitung ihrer personenbezogenen Daten*** aufgrund ihrer **besonderen Situation widersprechen.**

*PRAKTISCHES BEISPIEL:*
Widerspruch gegen die Verwendung von Informationen in Bezug auf ihr Privatleben (Namen der Kinder, Familienstand etc.) für Umfragezwecke, Widerspruch gegen eine Profilerstellung

## ACHTUNG:

**DIE ANTWORT MUSS ZWINGEND INNERHALB VON 1 MONAT AB DER ANFRAGE DURCH DIE BETROFFENE PERSON* ERFOLGEN (HÖCHSTENS 2 MONATE, WENN DIES DER BETROFFENEN PERSON* UNTER ANGABE EINER BEGRÜNDUNG MITGETEILT WIRD).**

**Der für die Verarbeitung Verantwortliche* muss einen Identitätsnachweis der betroffenen Person* verlangen.**

**Der Auftragsverarbeiter* muss den für die Verarbeitung Verantwortlichen* bei der Beantwortung der Fragen der betroffenen Person* unterstützen** ***(siehe Merkblatt 10 „Meldung von Datenschutzverletzungen“).***

** siehe Merkblatt 15 „Definitionen“*

REF-DE: 12/2017

# WELCHE RECHTE HABEN DIE BETROFFENEN PERSONEN?

7

**Dies** gilt nicht für bestimmte außerordentliche Fälle, in denen ein berechtigtes Interesse von Seiten des für die Verarbeitung Verantwortlichen* besteht.

*PRAKTISCHES BEISPIEL:*
Die gesetzliche Pflicht des für die Verarbeitung Verantwortlichen* zur Verarbeitung von PD*, zum Beispiel die Pflicht des Arbeitgebers, mitarbeiterbezogene PD* an die Finanzbehörden und Sozialversicherungsträger zu übermitteln

## RECHT AUF LÖSCHUNG („RECHT AUF VERGESSENWERDEN“)

Auf Verlangen der betroffenen Person* müssen alle ihre PD* aus der Datenbank gelöscht werden. Dies gilt für folgende Fälle:

- **Widerruf der Einwilligung**

*PRAKTISCHES BEISPIEL:*
„Ich möchte keine Werbemitteilungen mehr erhalten.“

- Eine **gesetzliche Pflicht**
  Manche gesetzliche Bestimmungen sehen vor, dass PD* nach Ablauf einer bestimmten Zeit nach ihrer Erhebung gelöscht werden müssen.

**ACHTUNG:**

**DER FÜR DIE VERARBEITUNG VERANTWORTLICHE* MUSS NACHWEISEN, DASS RECHTMÄSSIGE ZWINGENDE GRÜNDE FÜR DIE VERARBEITUNG* BESTEHEN, DIE VORRANG VOR DEN RECHTEN DER BETROFFENEN PERSON* HABEN.**

- PD* sind für den **Zweck* der Verarbeitung* nicht mehr erforderlich.**

*PRAKTISCHES BEISPIEL:*
Die Lieferung der Bestellung ist abgeschlossen.

- Die PD* wurden **ohne rechtliche Grundlage verarbeitet.**

*PRAKTISCHES BEISPIEL:*
Die PD* wurde für einen Zweck* verwendet, für den die betroffene Person* keine Einwilligung erteilt hat.

**ANMERKUNG:**

**MANCHMAL IST EINE LÖSCHUNG VON PD* AUFGRUND GESETZLICHER AUFBEWAHRUNGSPFLICHTEN NICHT MÖGLICH.**

*PRAKTISCHES BEISPIEL:*
Rechnung müssen zehn Jahre aufbewahrt werden.

## ÜBERMITTLUNG PERSONENBEZOGENER DATEN* AN DRITTE

Wenn eines dieser Rechte ausgeübt wurde und die PD* an einen Dritten außerhalb der Gruppe übermittelt wurden, **ist es ratsam, diesen Dritten davon in Kenntnis zu setzen.**

*PRAKTISCHES BEISPIEL:*
Wenn die PD* von dem für die Verarbeitung Verantwortlichen* gelöscht werden, muss auch der Dritte sie löschen.

** siehe Merkblatt 15 „Definitionen“*



REF-DE: 12/2017

# WELCHE RECHTE HABEN DIE BETROFFENEN PERSONEN ?

7

## RECHT AUF DATENÜBERTRAGBARKEIT

Die betroffene Person* hat ein Recht darauf, dass ihm seine Daten in einem **allgemein verwendeten Format** übermittelt werden. Dadurch kann die betroffene Person* ihre Daten leichter einem Wettbewerber übermitteln, der die gleiche Verarbeitung* durchführt.

**Welche PD*?**

- Alle elektronisch verarbeiteten PD* (Ausschluss der Papierverarbeitung)
- Nur von der betroffenen Person* mitgeteilte PD*, nicht solche, die das Unternehmen vervollständig hat
- Nur PD*, die aufgrund einer Einwilligung oder zur Erfüllung eines Vertrags oder im Vorfeld der Erfüllung eines Vertrags erhoben wurden

***PRAKTISCHES BEISPIEL:***

Erstellung einer elektronischen Kundenakte durch ein Vertriebsunternehmen.

Eine betroffene Person* bittet um Auskunft zu den Angaben, die sechs Monate zuvor in einem Formular für die Kundenakte mitgeteilt wurden: Name, Vorname, Anschrift, Telefonnummer, E-Mail-Adresse. Alle diese Angaben müssen der betroffenen Person* auf Anfrage übermittelt werden.

Andererseits müssen Informationen zu den Produkten, die die betroffene Person erworben hat oder zu den Vorlieben, die das Unternehmen daraus ermittelt hat, nicht in das zu übertragene Datenpaket eingeschlossen werden.

**INFORMATION:**

**Die Gruppe plant die Veröffentlichung eines Leitfadens zum Auskunftsverfahren.**

**ACHTUNG:**

- **DATENLÖSCHUNGEN**
- **DATENBERICHTIGUNGEN**
- **EINSCHRÄNKUNGEN DER VERARBEITUNG VON PD***

**MÜSSEN DER BETROFFENEN PERSON* MITGETEILT WERDEN.**

** siehe Merkblatt 15 „Definitionen“*

LEITFADEN PERSONENBEZOGENE DATEN


# INFORMATION DER BETROFFENEN PERSON

SAINT-GOBAIN

# INFORMATION
# DER BETROFFENEN PERSON

8

## WELCHE INFORMATION MUSS DER FÜR DIE VERARBEITUNG VERANTWORTLICHE* DER BETROFFENEN PERSON* MITTEILEN?

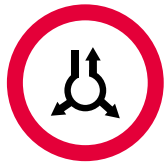
- Die **Identität** des für die Verarbeitung Verantwortlichen*
- Den **Zweck*** des Verarbeitungsvorgangs*
- Den **Empfänger** der personenbezogenen Daten*
- Die **Speicherdauer** der PD*
- Die **Rechte** der betroffenen Person* *(siehe Merkblatt 7 „Rechte der betroffenen Personen“)*
- Die Nutzung von **automatisierten Entscheidungssystemen** (falls zutreffend)
- **Gesetzliche Pflichtmeldungen** von PD* oder Daten, die für die **Erfüllung des Vertrags erforderlich** sind
- **Übermittlungen außerhalb der EU*** (falls zutreffend) *(siehe Merkblatt 9)*

## WANN MUSS DIE BETROFFENE PERSON INFORMIERT WERDEN?

- Vor der Verarbeitung* der PD* sowie während des gesamten Verarbeitungszeitraums

## WIE MUSS DIE INFORMATION ERFOLGEN?

- Zum Beispiel unter Berufung auf die **Datenschutzrichtlinie*** mit Hilfe eines Links zur Website
- Durch die Verwendung von durch die Europäische Kommission vorgeschlagenen **Piktogrammen**, z.B.

| PIKTOGRAMME | WESENTLICHE INFORMATION |
|---|---|
|  | Es werden nur solche personenbezogene Daten **erhoben**, die für den jeweiligen Verarbeitungszweck erforderlich sind. |
|  | Personenbezogene Daten werden nur jeweils für den Zweck **verwendet**, für den sie erhoben wurden. |

REF-DE: 12/2017

** siehe Merkblatt 15 „Definitionen“*

LEITFADEN PERSONENBEZOGENE DATEN


# INTERNATIONALE ÜBERMITTLUNG PERSONEN-BEZOGENER DATEN

SAINT-GOBAIN

# INTERNATIONALE ÜBERMITTLUNG PERSONENBEZOGENER DATEN

9

## WAS IST EINE ÜBERMITTLUNG?

- Eine Mitteilung, Kopie oder Verschiebung von PD* über ein Netzwerk

*PRAKTISCHES BEISPIEL:*
**Fernzugang**
Fernwartung aus Indien von PD* in der EU

*PRAKTISCHES BEISPIEL:*
**Übertragung von einem Medium auf ein anderes**
Von einer Festplatte auf einen Server, Memory Stick oder Computer etc.

## WAS BEDEUTET INTERNATIONAL?

- Wenn sich der Empfänger außerhalb der EU* befindet

## DER RICHTIGE REFLEX

*Unterscheidung von EU*- und Nicht-EU*-Situationen*

- Beachten Sie das vorliegende Merkblatt bei Übermittlungen außerhalb der EU*.
- Bei Übermittlungen innerhalb eines Landes (z.B. Deutschland) oder innerhalb der EU* (z.B. Deutschland-Frankreich) gelten die Regeln für internationale Übermittlungen nicht.

## EINE INTERNATIONALE ÜBERMITTLUNG IST NUR UNTER BESTIMMTEN BEDINGUNGEN MÖGLICH

- **Übermittlung an Länder mit einem angemessenen Datenschutzniveau** *(siehe Karte auf der nächsten Seite)*

*PRAKTISCHES BEISPIEL:*
Israel, Schweiz, Argentinien, Kanada

- **In die USA, wenn das importierende Unternehmen dem EU-Privacy Shield beigetreten ist**
- **Oder wenn die Übermittlung von angemessenen Zusicherungen begleitet wird:**
  - Unterzeichnung der Mustervertragsklauseln der Europäischen Kommission
  - Verbindliche Unternehmensregeln innerhalb des importierenden Unternehmens
  - Einwilligung der betroffenen Person*

## ACHTUNG

**DIE SAINT-GOBAIN-UNTERNEHMEN IN DEN USA SIND NICHT DEM EU-PRIVACY SHIELD BEIGETRETEN.**

## DER RICHTIGE REFLEX

1 - Prüfen Sie, ob der Auftragsverarbeiter* über verbindliche Unternehmensregeln verfügt oder in einem Land ansässig ist, das über ein ausreichendes Datenschutzniveau verfügt oder dem Datenschutzschild beigetreten ist.

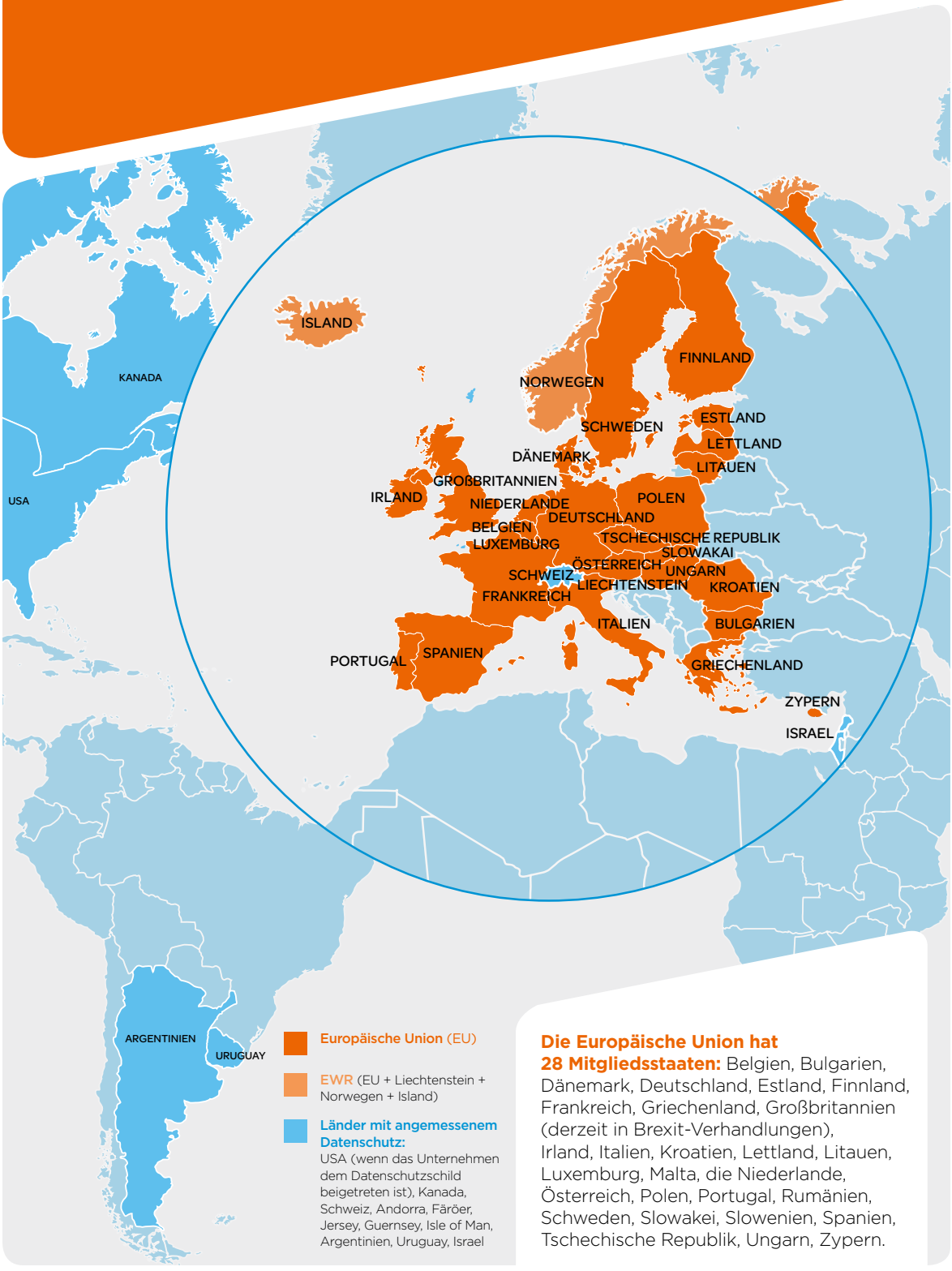
2 - Kontaktieren Sie ansonsten bitte Ihren Datenschutzbeauftragten.

** siehe Merkblatt 15 „Definitionen"*

REF-DE: 12/2017

# INTERNATIONALE ÜBERMITTLUNG PERSONENBEZOGENER DATEN

9




**Die Europäische Union hat 28 Mitgliedsstaaten:** Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Großbritannien (derzeit in Brexit-Verhandlungen), Irland, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, die Niederlande, Österreich, Polen, Portugal, Rumänien, Schweden, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Zypern.

REF-DE: 12/2017

LEITFADEN PERSONENBEZOGENE DATEN


# MELDUNG VON VERLETZUNGEN DES SCHUTZES PERSONEN-BEZOGENER DATEN

SAINT-GOBAIN

# MELDUNG VON VERLETZUNGEN DES SCHUTZES PERSONEN-BEZOGENER DATEN

10

## WAS IST EINE VERLETZUNG DES SCHUTZES PERSONEN-BEZOGENER DATEN?

- Eine **Verletzung des Schutzes** personenbezogener Daten (kurz: Datenschutzverletzung) ist ein Sicherheitsverstoß, der zu einem Verlust, einer Veränderung oder Weitergabe von PD* oder einem unbefugten Zugriff auf PD*, führt.
- Eine Datenschutzverletzung kann verschiedene Ursachen haben.

*PRAKTISCHES BEISPIEL:*
Ein Hackerangriff, der Verlust einer Festplatte, Softwarefehler etc.

- Risiken für die Rechte und Freiheiten der betroffenen Personen* müssen der Aufsichtsbehörde gemeldet werden.

## WER MACHT DIE MELDUNG?

- Das Unternehmen, das für die **Erhebung der PD*** verantwortlich ist, d.h. der für die **Verarbeitung Verantwortliche***

## AN WEN?

- An den **Landesdatenschutzbeauftragten** und
- An die betroffene Person* bei sensiblen Daten

## ACHTUNG

**Es kann sein, dass SAINT-GOBAIN über eine Datenschutzverletzung bei einem Auftragsverarbeiter*/Dienstleister nicht informiert ist!**

## WANN?

- Zwingend innerhalb von **72 Stunden** nach Kenntnis der Datenschutzverletzung oder nach Eingang einer Beschwerde einer betroffenen Person.

## WAS MUSS DIE MELDUNG BEINHALTEN?

- Die **Art** der betroffenen PD*
- Die **Kontaktdaten** des für die Verarbeitung Verantwortlichen*
- Die wahrscheinlichen **Folgen** der Datenschutzverletzung
- Die **Gegenmaßnahmen**, die ergriffen oder geplant wurden

**DOKUMENTIEREN SIE DATENSCHUTZVERLETZUNGEN STETS UND BEWAHREN SIE DIE UNTERLAGEN AUF.**

**DIE MELDUNG EINER DATENSCHUTZVERLETZUNG IST EINE HEIKLE ANGELEGENHEIT.**
Wenden Sie sich bitte sofort an den zuständigen Datenschutzbeauftragten*.

**DIE GRUPPE PLANT DIE VERÖFFENTLICHUNG EINES VERFAHRENS ZUR MELDUNG VON DATENSCHUTZVERLETZUNGEN.**

## DER RICHTIGE REFLEX:

**Schließen Sie in alle Verträge mit Auftragsverarbeitern* und Dienstleistern eine Verpflichtung zur Meldung von Datenschutzverletzungen ein.**

** siehe Merkblatt 15 „Definitionen"*

REF-DE: 12/2017

11

# WELCHE AUFSICHTSBEHÖRDE MUSS KONTAKTIERT WERDEN?

SAINT-GOBAIN

# WELCHE AUFSICHTSBEHÖRDE MUSS KONTAKTIERT WERDEN?

11

## PRINZIPIELL GILT: DIE ÖRTLICHE BEHÖRDE IST ZUSTÄNDIG.

- Zuständig ist die Aufsichtsbehörde des Mitgliedsstaates*, in dem das Unternehmen seinen Sitz oder seine Hauptverwaltung hat.
- Betroffene Personen*, deren personenbezogene Daten* einer Datenschutzverletzung ausgesetzt waren, können die Aufsichtsbehörde des Mitgliedsstaates* kontaktieren, in dem sie wohnen.

## PRAKTISCHE VORTEILE

- Nur ein zuständiger Ansprechpartner vor Ort
  **> Beschleunigung/Vereinfachung des Verfahrens**
- Eine Entscheidung für das gesamte EU*-Gebiet
  **> Einheitlichkeit**
- Die betroffene Person* kann sich **stets** an die Behörde des eigenen Mitgliedstaates* wenden, die dann ihrerseits die federführende Aufsichtsbehörde kontaktiert.

## AUSNAHME: DIE FEDERFÜHRENDE AUFSICHTSBEHÖRDE

Für **Unternehmen** bedeutet dieses Prinzip, dass sie nur mit einer einzigen Behörde zu tun haben, anstelle der **einzelnen Aufsichtsbehörden** in den **verschiedenen betroffenen Mitgliedstaaten**:

- bei Datenschutzverletzungen im Rahmen von Datenübermittlungen über Landesgrenzen hinweg

***PRAKTISCHES BEISPIEL:***
Ein Handwerker in Polen zeigt eine Datenschutzverletzung an, die PD* betrifft, welche von einem dänischen Unternehmen der SAINT-GOBAIN-Gruppe geschickt wurden. Die alleinige Zuständigkeit für die Gruppe liegt bei der französischen Datenschutzbehörde, aber der Handwerker, der eine natürliche Person ist, kann die polnische Aufsichtsbehörde kontaktieren, die in dieser Angelegenheit mit der französischen Datenschutzbehörde zusammenarbeiten wird.

- wenn mehrere Mitgliedstaaten* von der Datenschutzverletzung betroffen sind. Für SAINT-GOBAIN ist die federführende Aufsichtsbehörde die französische Datenschutzbehörde.
- für eine Unternehmen mit Sitz außerhalb der EU*, wenn der Verarbeitungsvorgang* Personen in mehreren Mitgliedstaaten* betrifft

** siehe Merkblatt 15 „Definitionen"*



REF-DE: 12/2017

LEITFADEN PERSONENBEZOGENE DATEN


# RISIKEN UND STRAFEN

SAINT-GOBAIN

# RISIKEN
# UND STRAFEN

12

## SANKTIONEN

### LEVEL 1 : NICHTBEACHTUNG DER REGELN

In Bezug auf:

- **Die Einwilligung von Kindern** unter 16 Jahren ist die Einwilligung des gesetzlichen Vertreters erforderlich
- **Verarbeitungsvorgänge*, die keine Identifizierung erfordern** unnötige Erhebung von PD*
- **Allgemeine Pflichten** des für die Verarbeitung Verantwortlichen*/ Auftragsverarbeiters*, insbesondere:
  - Datenschutz durch Technik *(siehe Merkblatt 4 „Technischer Datenschutz“)*
  - Führung eines Verzeichnisses
  - Sicherheit der PD*/der Verarbeitung
  - im Falle einer Datenschutzverletzung, Meldung an die Aufsichtsbehörde und ggf. an die betroffene Person
  - Durchführung einer Datenschutzfolgenabschätzung*
  - Einhaltung des Verhaltenscodex (verbindliche Unternehmensregeln*)

**Je nachdem, was höher ist:**
**€ 10.000.000** oder **2 %** weltweiten Vorjahresumsatzes SAINT-GOBAINs

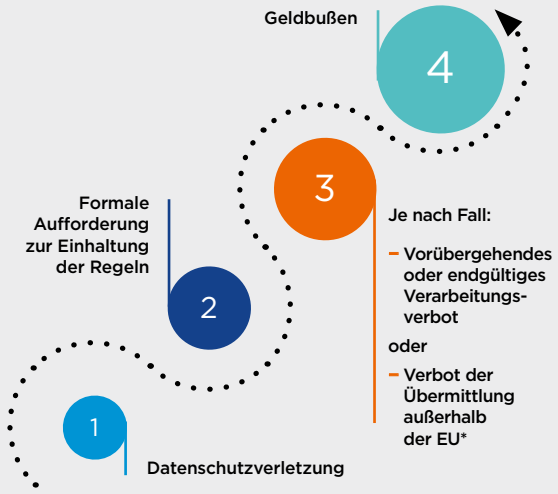
**ACHTUNG:**
DIE HÖHE DER **BUßGELDER** IST STARK **ANGESTIEGEN.**

### LEVEL 2 : NICHTBEACHTUNG DER REGELN

In Bezug auf:

- **Grundlegende Verarbeitungsprinzipien** (insbesondere: Einwilligung, Transparenz, Loyalität, Rechtmäßigkeit, Zweckbindung, Notwendigkeit, etc.)
- **Besondere Datenkategorien*/ sensible Daten*:** z.B. Angaben zu Rasse, politischen Meinungen, sexuellen Orientierung
- **Rechte der betroffenen Person*:** Information, Auskunft, Berichtigung, Löschung, Übertragbarkeit, Zweck, etc.
- **Übermittlung von PD* außerhalb der EU***
- **Verarbeitung*** im Rahmen des Arbeitsverhältnisses
- **Verfügungen und Ermittlungen** durch die Datenschutzaufsichtsbehörde

**Je nachdem, was höher ist:**
**€ 20.000.000** oder **4 %** weltweiten Vorjahresumsatzes SAINT-GOBAINs




** siehe Merkblatt 15 „Definitionen“*



REF-DE: 12/2017

LEITFADEN PERSONENBEZOGENE DATEN


# DATENSCHUTZ-BEAUFTRAGTER (DSB)

SAINT-GOBAIN

# DATENSCHUTZBEAUFTRAGTER (DSB)

13

## WAS IST EIN DATENSCHUTZ-BEAUFTRAGTER?

Der Datenschutzbeauftragte kann entweder ein **Mitarbeiter des für die Verarbeitung Verantwortlichen*** oder ein **externer Dienstleister** sein, der den für die Verarbeitung Verantwortlichen* bzw. den Auftragsverarbeiter* sowie deren Mitarbeiter informiert und berät.

- Er überwacht die Einhaltung der Gesetzgebung* sowie des nationalem Rechts zum Datenschutz.
- Er berät den für die Verarbeitung Verantwortlichen* zu Fragen der Datenschutzfolgenabschätzung* und überwacht ggf. deren Umsetzung.
- Er ist Ansprechpartner für die zuständige Aufsichtsbehörde.
- Er kann für die Ausführung seiner Aufgaben als DSB nicht von seinem Arbeitgeber entlassen oder sonst wie benachteiligt werden.
- Er untersteht direkt der höchsten Geschäftsebene des für die Verarbeitung Verantwortlichen*, damit **seine Unabhängigkeit** und **Autonomie** gewährt ist.
- Er ist im Hinblick auf die Ausübung seiner Aufgaben zur **Wahrung des Berufsgeheimnisses** und **der Schweigepflicht** verpflichtet.
- Er ist Ansprechpartner für die betroffenen Personen* bei allen **Fragen zur Verarbeitung* ihrer personenbezogener Daten* und zur Ausübung ihrer Rechte**.
- Er darf gleichzeitig auch andere Aufgaben übernehmen. Das Unternehmen muss jedoch sicherstellen, dass dadurch **keine Interessenkonflikte** entstehen.

## IN WELCHEN FÄLLEN MUSS EIN DSB ERNANNT WERDEN?

Die Ernennung eines DSB ist in folgenden Fällen Pflicht:

- Unternehmen, die aufgrund ihrer Haupttätigkeit regelmäßig, systematisch und in großem Umfang betroffene Personen* überwachen (z.B. Telefondienstleistungen, Geo-Tracking per mobile Apps)
- Unternehmen, die aufgrund ihrer Haupttätigkeit in großem Umfang sogenannte „sensiblen Daten“ verarbeiten (z.B. Krankenversicherungen, Krankenhäuser, Polizei, Sicherheitsdienste)

**DIE ERNENNUNG EINES DSB WIRD VOM GESETZGEBER NACHDRÜCKLICH EMPFOHLEN. DADURCH WIRD DIE FESTLEGUNG UND KOORDINATION VON DATENSCHUTZMASSNAHMEN EINEM AUSGEWIESENEN FACHMANN ANVERTRAUT.**

## WER KANN DSB WERDEN?

Personen, die aufgrund ihrer **beruflichen und fachlichen Fähigkeiten, insbesondere ihrer Kenntnisse in Bezug auf Recht, Informatik und den Geschäftsprozess ausgewählt werden**. Die ernannte Person sollte die **Sprache des Landes ihres Zuständigkeitsbereichs sprechen**.

## WELCHE PFLICHTEN HAT DAS UNTERNEHMEN?

- Es muss dafür sorgen, dass der DSB bei jeder Frage in Bezug auf den Schutz personenbezogener Daten* **angemessen** und **zeitnah einbezogen wird**.
- Es muss den DSB bei der Ausübung seiner Tätigkeit unterstützen, ihm die **notwendigen Mittel zur Verfügung gestellt werden**, und ihm Zugang zu den personenbezogen Daten* und den Verarbeitungsvorgängen* gewähren.
- Es muss dafür sorgen, dass der DSB bei der Erfüllung seiner Aufgaben **unabhängig** und **weisungsfrei** bleibt.

** siehe Merkblatt 15 „Definitionen“*

REF-DE: 12/2017

LEITFADEN PERSONENBEZOGENE DATEN


# DIE 5 GOLDENEN REGELN FÜR DIE VERARBEITUNG PERSONEN-BEZOGENER DATEN

SAINT-GOBAIN

# DIE 5 GOLDENEN REGELN FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN

14

1. **Die Verarbeitung* erfolgt mit einem konkreten Zweck:**
   - z.B.: die Zuordnung einer SGID für jeden Mitarbeiter der Gruppe.

2. **Die PD* werden abhängig von ihrem Zweck* für eine begrenzte Dauer aufbewahrt:**
   - z.B.: Bei Bezahlung im Internet werden die Kreditkartendaten des Kunden nur solange aufbewahrt, bis die Bezahlung abgeschlossen ist.

3. **Die betroffene Person* hat ein Auskunftsrecht, ein Informationsrecht und ein Recht auf Einschränkung der Verarbeitung*:**
   - Die Erhebung ist klar und eindeutig definiert.
   - Die betroffene Person* muss über ihr Recht auf Auskunft und Löschung informiert werden.
   - Verarbeitungsbeschränkung steht für die Verwendung erhobener PD* ausschließlich für einen bestimmten Prozess* unter Ausschluss aller anderen Prozesse*.
   - Die Verarbeitung* ist vertraulich und muss sicher sein.
   - Geeignete Maßnahmen müssen erfolgen, um die Verarbeitungssicherheit zu gewährleisten → Vermeidung von Datenschutzverletzungen

4. **Die Erhebung von PD* ist relevant:**
   - Nur PD*, die für den Verarbeitungszweck* unbedingt erforderlich sind, werden erhoben.

5. **Der für die Verarbeitung Verantwortliche* gewährleistet die Sicherheit und Vertraulichkeit der PD*.**
   - Verwendung technischer Maßnahmen: z.B. Serversicherheit, Intrusion-Prevention-Tools
   - Die Offenlegung von PD* gegenüber Dritten ist verboten.

REF-DE: 12/2017

** siehe Merkblatt 15 „Definitionen“*

15

# DEFINITIONEN

SAINT-GOBAIN

# DEFINITIONEN

15


- **Anonymisierung:** Technik, die darin besteht, aus einem Satz von PD alle Merkmale zu eliminieren, die eine Identifizierung der jeweiligen Person ermöglichen
- **Verbindliche Unternehmensregeln:** Verhaltenscodex, der die internationalen Übermittlung von PD definiert. Sie bieten einen geeigneten Schutz für PD, die aus einem EU-Land in ein Drittland übermittelt werden.
- **Für die Verarbeitung Verantwortlicher:** Unternehmen, in dessen Namen die Verarbeitung erfolgt
- **Betroffene Person:** die Person, deren Daten erhoben werden
- **Auftragsverarbeiter:** eine natürliche oder juristische Person, die PD im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet
- **Mitgliedsstaat:** bezeichnet einen der 28 EU-Staaten
- **OPT IN:** Einholung der Zustimmung der betroffenen Person vor der Verarbeitung. Wenn die Person nicht „Ja“ sagt, bedeutet dies „Nein“.
- **OPT OUT:** Das Gegenteil von OPT IN: Wenn die Person nicht „Nein“ sagt, bedeutet dies „Ja“. Bei OPT OUT kann die Zustimmung jederzeit widerrufen werden.
- **Personenbezogene Daten/„PD“:** sämtliche Informationen, die es ermöglichen, eine Person direkt oder indirekt zu bestimmen; es handelt sich daher um eine personenbezogene Information, sobald die Person bestimmt werden kann oder sie bestimmbar wird.
- **Datenschutzbeauftragter:** Die Person bei SAINT-GOBAIN, die in Bezug auf eine oder mehrere Unternehmen für die Einhaltung der jeweiligen Datenschutzgesetzgebung zuständig ist. Er ist Ansprechpartner bei einem Verstoß gegen Datenschutzbestimmungen.
- **Datenschutzrichtlinie:** Die Richtlinie zur Verarbeitung von PD innerhalb der SAINT-GOBAIN-Gruppe
- **Datenschutzschild:** Übereinkommen zwischen der EU und den USA zum Datenschutz, dem jedes US-Unternehmen beitreten kann
- **Verarbeitung oder Verarbeitungsvorgang:** Jeder Vorgang oder jede Vorgangsreihe, der PD betrifft, unabhängig von der Art des Verarbeitungsverfahrens (Erhebung, Erfassung, Organisation, Speicherung, Anpassung, Veränderung, Entnahme, Abfrage, Nutzung, Weitergabe durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Verknüpfung, Einschränkung, Blockierung, Löschung oder Vernichtung etc.) -> was mit den PD geschieht
- **Pseudonymisierung:** Technik, die darin besteht, ein bestimmendes Merkmal oder einen Teil der PD durch eine Pseudonym zu ersetzen. Dieser Vorgang ist umkehrbar, so dass eine Bestimmbarkeit der Person wieder möglich gemacht werden kann.
- **Gesetzgebung:** Bezeichnet die Europäische Datenschutzverordnung sowie die Datenschutzgesetze der einzelnen Mitgliedsstaaten.
- **Besondere Kategorien personenbezogener Daten/sensible Daten:** Personenbezogene Daten, deren Verarbeitung eine Gefahr für die Rechte und Freiheiten der betroffenen Person darstellen können, z.B. politische oder religiöse Meinungen, sexuelle Vorliegen, medizinische Daten etc.

REF-DE: 12/2017