DSGVO Umsetzung mittels online Tool

1 Jahr danach

Intervalid | DSGVO Software

Intervalid GmbH | info@intervalid.com | www.intervalid.com

Intervalid GmbH

ein kurzes „wir über uns“

- 2016: Start Software-Entwicklung
- 2017: Firmengründung
- 2018: Eröffnung Standort DE
- 2019: > 300 mittelständische bis Großkunden sowie externe Datenschutzbeauftragte

Bayerisches Landesamt für Datenschutzaufsicht

BayLDA | Online-Services | Datenschutz | Veröffentlichungen | Unsere Behörde | Suche...

> Datenschutz > Datenschutzprüfungen

Datenschutzprüfungen

Das BayLDA führt im Rahmen seiner gesetzlichen Aufgaben regelmäßig anlassbezogene und anlasslose Datenschutzprüfungen durch. Anlassbezogene Prüfungen erfolgen meist aufgrund von Beschwerden oder konkreten Hinweisen auf mögliche Datenschutzverstöße. Anlasslose Prüfungen erfolgen nach pflichtgemäßem Ermessen branchenunabhängig in allen Regionen Bayerns. Das BayLDA führt diese anlasslosen Prüfungen in der Regel als sog. fokussierte Prüfungen bei einzelnen Unternehmen vor Ort, als Prüfungen im Wege eines schriftlichen Verfahrens oder als Onlineprüfung automatisiert über das Internet durch. Darüber hinaus beteiligt sich das BayLDA auch an überregionalen Prüfungen.

Im nachfolgenden Bereich ist eine Auswahl der vom BayLDA durchgeführten Kontrollen aufgelistet.

Datenschutzprüfungen		
03/2019		
Löschen von Daten bei ERP-Systemen (SAP)	Status: Anstehend	
Datenschutzverletzungen bei (Unter-)Auftragverarbeitern	Status: Anstehend	
11/2018		
Patch Management WordPress – WP GDPR Compliance Plugin	Status: Läuft	
Umsetzung der DS-GVO bei kleinen und mittelständischen Unternehmen (KMUs)	Status: Läuft	
10/2018		
Patch Management eCommerce-Systeme/Online-Shops (Magento)	Status: Läuft	
Informationspflichten in Bewerbungsverfahren	Status: Läuft	
Ransomware bei Arztpraxen	Status: Läuft	
Rechenschaftspflicht bei Großkonzernen	Status: Läuft	
02/2018		

Datenschutzprüfungen (Auszug Prüfkatalog)

Bayerisches Landesamt für Datenschutzaufsicht

Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO)

9. Ist ein vollständiges Verarbeitungsverzeichnis vorhanden?
   - ☐ Ja. Anzahl der Verarbeitungstätigkeiten:_____
   - ☐ Nein. Grund:_____

10. Beschreiben Sie bitte kurz (ca. 1 Seite), nach welcher Methode (z.B. Zweck, Mittel, Prozess, IT-System, Abstraktion, ...) die einzelnen Verarbeitungstätigkeiten ermittelt werden.

11. Sind bei den Empfängern auch interne Stellen (z.B. Personal, Geschäftsleitung, Marketing,...) umfasst?
   - ☐ Ja.
   - ☐ Nein. Grund:_____

12. Beschreiben Sie bitte kurz (ca. 1 Seite) die Regelungen, wie das Verarbeitungsverzeichnis verwaltet (z.B. aktualisiert) wird?

Datenschutzprüfungen (Auszug Prüfkatalog)

Bayerisches Landesamt für Datenschutzaufsicht

10. Existiert ein Löschkonzept (z.B. nach DIN 66398), das auch den Umgang mit Archiven und Backups regelt?

☐ Ja. Bitte senden Sie uns eine Kopie dieses Konzepts zu.

☐ Nein. Grund:_____

Datenschutzprüfungen (Auszug Prüfkatalog)

Bayerisches Landesamt für Datenschutzaufsicht

12. Sind die Beschäftigten zur weisungsgebundenen Verarbeitung personenbezogener Daten in ihrem Arbeitsbereich sensibilisiert und verpflichtet (Art. 29 DS-GVO)?

☐ Ja. Bitte senden Sie uns ein Muster zu.

☐ Nein. Grund:_____

18. Sind Schulungsunterlagen vorhanden, mit denen die Personen, die an den Prozessen zur Sicherstellung der Betroffenenrechte mitarbeiten, sachgerecht informiert werden.

☐ Ja. Senden Sie uns bitte eine Kopie dieser Unterlagen zu.

☐ Nein. Grund:_____

Datenschutzprüfungen (Auszug Prüfkatalog)

Bayerisches Landesamt für Datenschutzaufsicht

3. Sind, falls Sie einen Datenschutzbeauftragten haben, die letzten (zwei) Audits des Datenschutzbeauftragten vorhanden und besitzen diese eine einheitliche Prüfmethodik?

☐ Ja. Bitte senden Sie uns Kopien der Prüfberichte zu.

☐ Nein. Grund:_____

☐ Wir haben keinen Datenschutzbeauftragten.

11. Werden geeignete Security-Maßnahmen zur Sicherstellung der Verfügbarkeit, Vertraulichkeit und Integrität nach Art. 32 DS-GVO getroffen?

☐ Ja. Bitte senden Sie uns bitte das IT-Sicherheitskonzept bzw. eine Zusammenfassung davon zu.

☐ Nein. Grund:_____

Datenschutzprüfungen (Auszug Prüfkatalog)

Bayerisches Landesamt für Datenschutzaufsicht

19. Wie viele Datenschutzverletzungen nach Art. 33/34 DS-GVO sind bei Ihnen bekannt geworden?

☐ Anzahl seit 25.05.2018:_____

☐ Keine

20. Gibt es einen (dokumentierten) Prozess, um Datenschutzverletzungen innerhalb 72 Stunden (auch an Wochenenden/Feiertagen) bei der zuständigen Aufsichtsbehörde zu melden?

☐ Ja.

☐ Nein. Grund:_____

Erfahrungen aus Kundenprojekten
Herausforderungen bei der Umsetzung

Aus den bisherigen Projekten

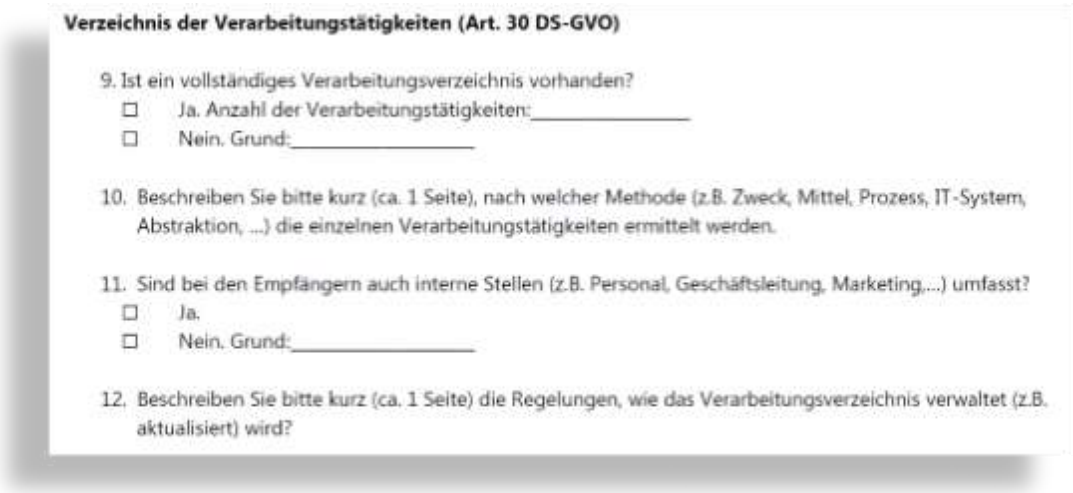
- Fachbereich aktiv einbinden (Akzeptanz)
- Excel aktuell halten, verteilen im Unternehmen und in Konzernstrukturen
- Datenqualität (Inhalt, auswertbar?)
- Nachvollziehbarkeit (Protokollierung von Änderungen, neuen Systemen)
- Freigabe durch DSB
- Status bei den Tochtergesellschaften? Mustervorgaben helfen
- Mehrsprachigkeit (Konzernsprache|Landessprache)
- Aufgaben verteilen, evident halten
- Lückenlose Bearbeitung aller DSGVO Themen an einem Ort
- Wartung bei gesetzlichen Änderungen

Das Verzeichnis aktuell und richtig halten mittels online Tool

- Workflow für ein aktuelles Verzeichnis

  Punktuell bei Änderungen in Ihrer Organisation

  – **Neue** Verarbeitung/Auftragsverarbeitung im Unternehmen
  – **Ändern** einer Verarbeitung
  – (Jährliche) Überprüfung des **gesamten** Verzeichnisses



Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO)

9. Ist ein vollständiges Verarbeitungsverzeichnis vorhanden?
   - ☐ Ja. Anzahl der Verarbeitungstätigkeiten:_____
   - ☐ Nein. Grund:_____

10. Beschreiben Sie bitte kurz (ca. 1 Seite), nach welcher Methode (z.B. Zweck, Mittel, Prozess, IT-System, Abstraktion, ...) die einzelnen Verarbeitungstätigkeiten ermittelt werden.

11. Sind bei den Empfängern auch interne Stellen (z.B. Personal, Geschäftsleitung, Marketing,...) umfasst?
   - ☐ Ja.
   - ☐ Nein. Grund:_____

12. Beschreiben Sie bitte kurz (ca. 1 Seite) die Regelungen, wie das Verarbeitungsverzeichnis verwaltet (z.B. aktualisiert) wird?

Das Verzeichnis aktuell und richtig halten

- Workflow für neue Verarbeitungen und Änderungen
  - Mitarbeiter aktiv einbinden
  - Beliebige User anlegen
  - Änderungen, neue Verarbeitungen einfach erfassen
  - Fragebogen auf Wunsch ausfüllen
  - Zur Freigabe (4-Augen-Prinzip) an den DSB weiterleiten
  - Protokoll ansehen und Verzeichnis aktualisieren

- Fokus auf Transparenz, Aktualität, Nachvollziehbarkeit

Ersterhebung Bewerberverwaltung

Beispiel Workflow: eine neue Verarbeitung erfassen

24.09.2019 10:47:04

Ersterhebung erfasst
Corinna Bachner

24.09.2019 10:47:10

Weitergeleitet
Von Corinna Bachner an Sonja Rothenheim

Allgemeine Information zur Verarbeitung

Für die Ersterhebung werden alle Verarbeitungstätigkeiten erfasst. Darunter fällt jede Art der Verarbeitung personenbezogener Daten; der Bezug zu einer Person ist gegeben. Beispiel: Personen bei einem Kunden, Interessenten, Partner und auch Mitarbeiter, Bewerber. Die Verarbeitung kann in einer Software, im Excel oder auch auf Papier sein (sofern es sich hier um eine strukturierte Sammlung handelt.

Was ist die geläufige Bezeichnung für diese Verarbeitungstätigkeit?

Bewerberverwaltung

Beschreibung

Beschreibung

Für welchen Zweck wird die Verarbeitung durchgeführt?

Verwendung und Evidenthaltung von personenbezogenen Daten von Bewerbern für die

Öffne Kommentare

Änderung Digitaler Personalakt

Beispiel Workflow: eine Verarbeitung ändern

Allgemeine Informationen

24.09.2019 10:30:07

Änderung gestartet
Corinna Bachner

24.09.2019 10:32:13

Weitergeleitet
Von Corinna Bachner an Sonja Rothenheim

Unternehmen (Pflicht)

Muster Unternehmen

Bezeichnung (Pflicht)

Digitaler Personalakt

Beschreibung

Beschreibung

Zweck (Pflicht)

Verwaltung von unternehmensrelevanten Dokumenten und Informationen in Zusammenhang mit Personaladministration und -abrechnung. Elektronische Ablage der Dienstverträge und Vertragsunterlagen zum Beschäftigungsverhältnis.

Verwaltung von unternehmensrelevanten Dokumenten und Informationen in Zusammenhang mit Personaladministration und -abrechnung.

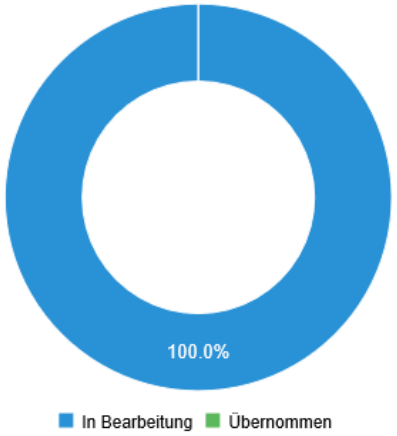
Öffne Kommentare

Das Verzeichnis aktuell und richtig halten

- Regelmäßige (halbjährlich, jährliche) Überprüfung des Verzeichnisses
  - Nachkontrolle starten und Mitarbeiter informieren
  - Kontrolle durch Fachbereich
  - Zur Freigabe (4-Augen-Prinzip) an den DSB weiterleiten
  - Änderungen sind ersichtlich
  - Ins Verzeichnis übernehmen – protokolliert

12. Beschreiben Sie bitte kurz (ca. 1 Seite) die Regelungen, wie das Verarbeitungsverzeichnis verwaltet (z.B. aktualisiert) wird?

Fortschritt



Kontrolle

Prüfung Verzeichnis der Verarbeitungstätigkeiten nach Artikel 30 DSGVO. Regelmäßige Überprüfung der Aktualität und Richtigkeit des Verzeichnisses.

Beginn: 09.08.2019

Ende: Ende

Nachkontrolle abschließen | Zurück

Starte Nachkontrolle oder leite diese weiter.

Verarbeitungen hinzufügen

Hier können Sie das Verzeichnis intern zur Kontrolle weiterleiten.
1. Überprüfen und ergänzen Sie die zuständigen User in der Spalte "Wird geprüft von".
2. Wählen Sie die Verarbeitungstätigkeiten aus, für die Sie eine Aktion starten wollen.
3. Wählen Sie die gewünschte Aktion

Alle selektieren | Suchbegriff | Suchen | Aktion wählen

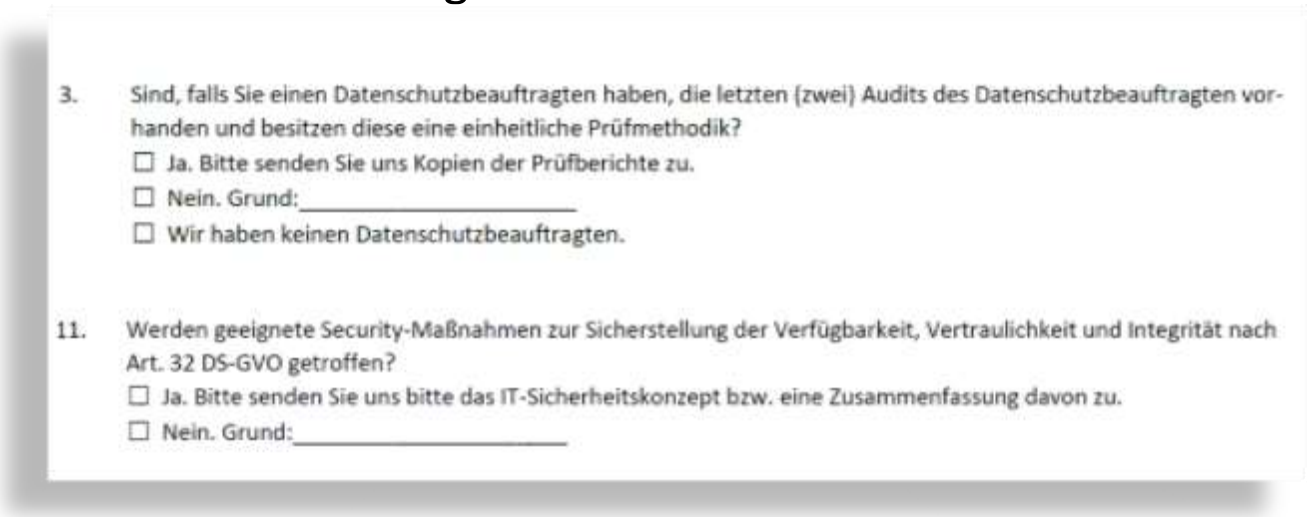
Finanz-und Rechnungswesen	Fortschritt		Status	Wird geprüft von:
Muster Unternehmen	Fertig	Muster Inventarliste Arbeitsmittel	Zurückgesendet von Corinna Bachner	Corinna Bachner
Muster Unternehmen	In Bearbeitung	Muster Rechnungswesen	Weitergeleitet an Corinna Bachner	Corinna Bachner
IT				
Muster Unternehmen	In Bearbeitung	Muster Benutzerverwaltung		Sonja Rothenheim

Sicherheit gewährleisten
Vertraulichkeit, Verfügbarkeit, Integrität

- Audits und Sicherheitsmaßnahmen

  Prüfungen durchführen

  – Checklisten aussenden, Informationen einholen
  – Ergebnisse auswerten, Gaps identifizieren
  – Maßnahmen setzen, Aufgaben abarbeiten
  – Management report
  – Umfragen durchführen



3. Sind, falls Sie einen Datenschutzbeauftragten haben, die letzten (zwei) Audits des Datenschutzbeauftragten vorhanden und besitzen diese eine einheitliche Prüfmethodik?
   ☐ Ja. Bitte senden Sie uns Kopien der Prüfberichte zu.
   ☐ Nein. Grund:_____
   ☐ Wir haben keinen Datenschutzbeauftragten.

11. Werden geeignete Security-Maßnahmen zur Sicherstellung der Verfügbarkeit, Vertraulichkeit und Integrität nach Art. 32 DS-GVO getroffen?
   ☐ Ja. Bitte senden Sie uns bitte das IT-Sicherheitskonzept bzw. eine Zusammenfassung davon zu.
   ☐ Nein. Grund:_____

Audits : Checklisten weiterleiten Gaps identifizieren

Ergebnisse im Detail anzeigen

Zurück

Filter

Konform | Risiko | Hohes Risiko | Nicht beurteilbar

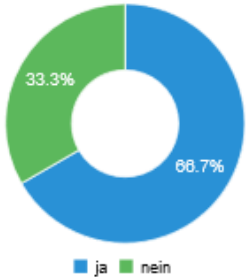
Aufgaben: Alle | Verarbeitungstätigkeit: Alle | Erstelle Report ...

Muster Kundenbetreuung und Marketing (CRM) im B2B Bereich | Checkliste Verarbeitung

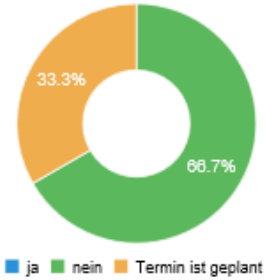
Datenschutz-Grundsätze	Werden Daten nur so lange gespeichert, wie sie zur Erreichung des Zwecks benötigt werden (Speicherbegrenzung)?	- Nein, Daten werden derzeit nicht gelöscht	1	
Vertraulichkeit	Wie wird das unbefugte Kopieren von personenbezogene Daten abgesichert?	- Nein, derzeit Export und Kopieren möglich	Keine Aufgaben	
Vertraulichkeit	Ist sichergestellt, dass bei einem externen Fernzugriff auf die Anwendung durch z.B. den Hersteller (Support) die nötige Vereinbarung zur Auftragsdatenverarbeitung getroffen wurde?	- Noch offen, derzeit noch nicht im Vertrag vorgesehen-	Keine Aufgaben	
Vertraulichkeit	Sind Abfragen und Auswertungen eingeschränkt verfügbar und abgesichert?	- Abfragen sind derzeit ohne Einschränkung verfügbar	Keine Aufgaben	
Schutz bei Übermittlung, Transport	Wie sind Daten bei der elektronischen Übertragung gesichert?	- Email ungesichert	Keine Aufgaben	
Informationspflicht	Werden die betroffenen Personen ausreichend informiert, wenn die personenbezogenen Daten bei der betroffenen Person erhoben wurden?	- In Arbeit	Keine Aufgaben	
Informationspflicht	Werden die betroffenen Personen im Falle der Erhebung der Daten bei der betroffenen Person zum Zeitpunkt der Erhebung der Daten informiert?	- In Arbeit	Keine Aufgaben	
Informationspflicht	Auf welche Weise werden die betroffenen Personen informiert?	- Schriftlich, Vorlage fehlt noch	Keine Aufgaben	

Entsorgung von internen und externen Unterlagen

Haben Sie die neue Richtlinie erhalten?



Ist das Thema in Ihrem regelmäßigen Jour fixe besprochen worden?

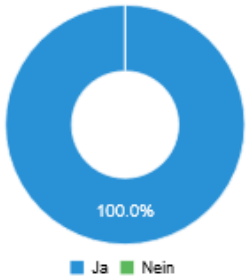


Umfragen :

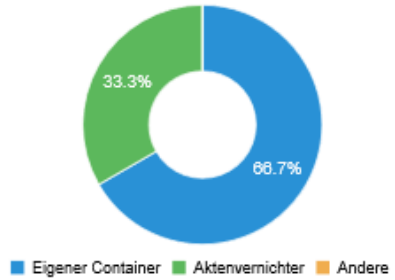
Greifen die Sicherheits-maßnahmen?

Kundenunterlagen entsorgen

Bekommen Sie Unterlagen von Kunden?

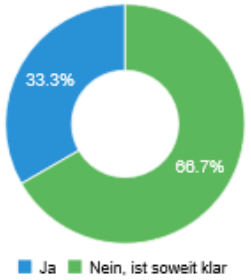


Wo werden diese derzeit entsorgt?



Weitere Fragen

Benötigen Sie Unterstützung bei der Umsetzung?



Haben Sie weitere Fragen?

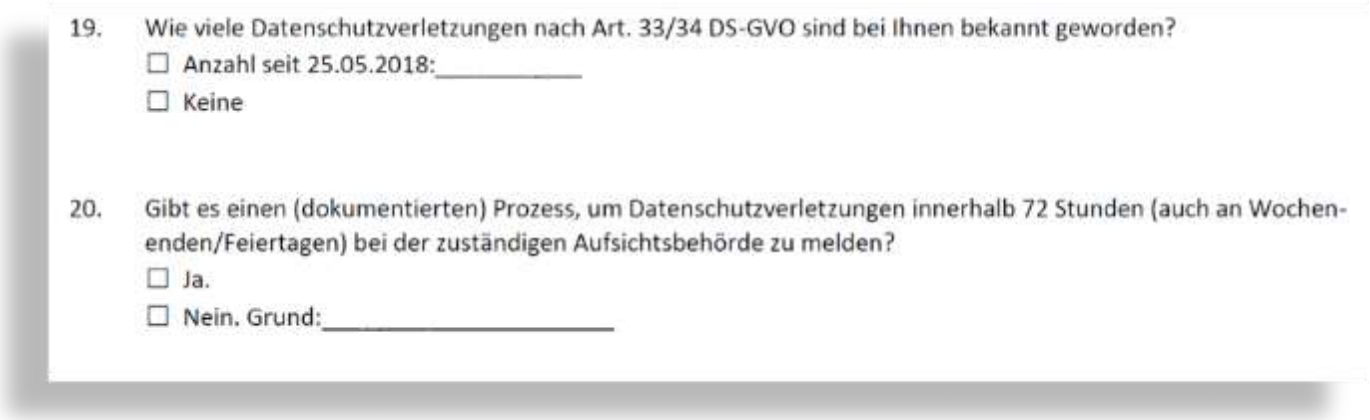
Ab wann gilt die Policy?

Wo werden USP Sticks entsorgt?

Wie gehe ich mit Emails vor, die Anhänge mit sensiblen Daten enthalten?

Der Umgang mit Datenschutzverletzungen

- Mit Datenpannen umgehen
  - Datenpannen festhalten, Mitarbeiter einbinden
  - Formular als Hilfestellung (welche Informationen sind wichtig)
  - Eskalation: weitere Stellen im Unternehmen informieren
  - Maßnahmen setzen, um Risiko jetzt und in Zukunft zu minimieren
  - Vorbereitung für die Meldung an die Behörde



19. Wie viele Datenschutzverletzungen nach Art. 33/34 DS-GVO sind bei Ihnen bekannt geworden?
☐ Anzahl seit 25.05.2018:_____
☐ Keine

20. Gibt es einen (dokumentierten) Prozess, um Datenschutzverletzungen innerhalb 72 Stunden (auch an Wochenenden/Feiertagen) bei der zuständigen Aufsichtsbehörde zu melden?
☐ Ja.
☐ Nein. Grund:_____

Data Breach

Erstelle Report ...

Erhebung - Information | Dokumentation | E-Mail senden

Fragebogen (Pflicht)

Data Breach Notification DE

Allgemeine Angaben

Was ist passiert?

- Cyberangriff
- Ransomware
- Malware
- Phishing
- Softwarefehler
- Skimming
- Diebstahl
- Verlust
- Fehlversendung
- Fehlentsorgung
- Fehlerhafte Löschung
- Sonstiges

Wo ist der Vorfall passiert?

Weitere Hilfestellung

Zusätzliche Funktionen

- Fragebögen aussenden
- Mitarbeiter Umfragen durchführen
- Schulungen dokumentieren
- E-Learning Anbindung
- Betroffenen Rechte erfüllen
- Datenfluss auswerten
- Reports
- TOMs, Folgeabschätzung

Sie haben Fragen?
Besuchen Sie uns am Stand 10.1. - 524 Wir beraten Sie gerne!

DE: +49 721 1608 1337
AT: +43 1 905 10 44
info@intervalid.com

Intervalid | DSGVO Software