Datenschutz- und Löschkonzept für die IOS2000 und DIALOG Warenwirtschaft auf Grund der neuen EU-Datenschutzgrundverordnung ab Mai 2018

Inhalt

Wichtiger Hinweis:

Alle diese Informationen in diesem Dokument sind ohne Gewähr und Anspruch auf Richtigkeit und Vollständigkeit. Für die Einhaltung der geltenden und kommenden Gesetze und Durchführungsverordnungen sind ausschließlich die Inhaber und Geschäftsführer verantwortlich.

Nehmen Sie unbedingt rechtzeitig professionelle (Rechts-)Beratung in Anspruch.

Vorwort

Am 25. Mai 2018 tritt ein neues, strenges Datenschutzrecht in Kraft.

Ab diesem Tag werden die Regelungen der Datenschutz-Grundverordnung (DSGVO) unmittelbar geltendes Recht in allen Staaten der Europäischen Union (EU). Damit wird ein einheitliches Datenschutzniveau in den Mitgliedstaaten gewährleistet. Die Wahlmöglichkeiten, welche die DSGVO vorsieht, hat Deutschland im Bundesdatenschutzgesetz (BDSG neu) ausgeübt. Das BDSG neu tritt ebenfalls am 25. Mai 2018 in Kraft.

Die Datenschutzaufsichtsbehörden erhalten zur Durchsetzung umfangreiche Befugnisse und haben demgemäß ihre Personalkapazitäten aufgestockt.

Flankiert werden die erweiterten Befugnisse durch eine Ausweitung des Bußgeldrahmens bei Verstößen. Bisher konnten max. 300.000 € als Bußgeld festgesetzt werden. Zukünftig sind Bußgelder bis 20 Millionen € oder 4 % vom Jahresumsatz zulässig, wobei der jeweils höhere Wert gilt.

Besonders, wenn Sie einen Internetshop betreiben oder Endkundendaten erfassen und verarbeiten, ist das für Sie von höchster Priorität!

Das neue Datenschutzrecht beinhaltet umfangreiche und detaillierte Pflichten für Unternehmen. Es müssen interne Prozesse angepasst und evtl. neu strukturiert werden. Auch eine Schulung Ihrer Mitarbeiter ist unerlässlich.

Haben Sie mehr als 10 Mitarbeiter, die mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (Auftragsbearbeitung, Kasse, Shop)? Dann brauchen Sie auf jeden Fall einen Datenschutzbeauftragten!

Die wichtigsten Regeln, die Sie konkret betreffen

Der Begriff ´personenbezogene Daten´ betrifft nach Definition der DSGVO in erster Linie alle Informationen, die die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Im Umkehrschluss sind Firmen davon ausgeschlossen, wobei auch hier natürlich die bestehenden Gesetze des Datenschutzes weiter gelten.

Will heißen, wenn Sie KEINE Daten von Privatpersonen, sondern nur von Firmen im B2B Wiederverkäufergeschäft erfassen, gilt die neue DSGVO nicht oder nur eingeschränkt für Sie.

Aber in dem Moment, wo Sie die erste private Adresse (von einem Endkunden, Hobbyschrauber usw.) erfassen und speichern, gilt die DSGVO für Sie in vollem Umfang!

Die wichtigsten Regeln kann man in etwa für Jedermann verständlich so zusammenfassen:

1. Es dürfen nur zweckgebundene Daten erfasst und gespeichert werden, die man für die Aufgabe, die ich mit diesen Daten erledigten will, brauche.

2. Der Betroffene hat ein uneingeschränktes Recht darauf, zu erfahren, was mit seinen Daten passiert, wo und wie sie gespeichert werden und ob und warum diese an Dritte weitergegeben

werden (was schon sehr bedenklich ist).

3. Der Betroffene hat ein Recht auf Löschung seiner Daten (mehr dazu später).

Den genauen Wortlaut und die Definitionen finden Sie z.B. gut verständlich im Artikel über die neue DSGVO bei Wikipedia unter dem Link:

https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung

oder natürlich im Original-Gesetzestext, den Sie in verschiedenen Variationen im Web finden.

Programmänderungen zur Unterstützung der DSGVO

Im Laufe der nächsten Updates ab Version 346 kommen einigen Änderungen.

Die Realisierung wird aber einige Versionen dauern, weil wir alle Suchergebnisse, unzählige Reports und Grids um die Selektion nach diesen neuen Kennzeichen erweitern müssen.

Datenschutzstufe im Benutzerstamm

Unabhängig von den Benutzerrechten, die Sie selbst abhängig von den Aufgabenbereichen und Vollmachten der Benutzer vergeben müssen, werden die Benutzerstammdaten um eine Datenschutz-Stufe ergänzt. Ist diese Datenschutzstufe auf 0 (Standard-Einstellung bei allen Benutzern), darf der Benutzer keinerlei Exporte oder Ausdrucke mehr von Listen und Grids machen, auf denen Kundendaten enthalten sind.

Verbraucherkennzeichen im Kundenstamm

Der Kundenstamm wird erweitert um ein Kennzeichen, ob es sich um einen (privaten) Endverbraucher oder um einen gewerblichen Kunden handelt.

Löschkennzeichen in den Stammdaten

Alle Stammdaten werden um ein neues Datenfeld ´Löschkennzeichen´ erweitert.

Wenn ein Benutzer mit Löschrechten dann den Datensatz löschen will, klickt er wie bisher auf den Löschbutton. Allerdings wird dann zuerst nur das Löschkennzeichen im Datensatz gesetzt auf ´Vormerkung zur Löschung´. Diese Aktion wird selbstverständlich protokolliert.

Das Löschkennzeichen kann dann im Laufe des Tages – allerdings nur von einem Benutzer mit Datenschutzkennzeichen 2 (Datenschutzbeauftragter) – wieder rückgängig gemacht werden, wenn die endgültige Löschung aus wichtigem Grund unterbunden werden soll.

Ansonsten wird der Datensatz nach den Regeln des nachfolgenden Löschkonzeptes in der nächsten Nacht bei einem automatischen Löschlauf gelöscht.

Export der Kundendaten

Sie werden in den Kundenstammdaten auf dem Zusatz-Tab einen neuen Button bekommen, mit dem Sie auf Anfrage des (End)Kunden alle meldepflichtigen Kundendaten in eine XML Datei exportieren und als verschlüsselte ZIP-Datei dem Kunden per Mail zusenden können. Sie müssen in diesem Fall nur mit dem Kunden ein Passwort vereinbaren.

Diese Datei wird neben den gespeicherten Stammdaten auch in der Datenbank gespeicherten Historie- und Umsatzeinträge (ohne Erlöse) des Kunden beinhalten.

Die Auslegung der DSGVO sagt, dass ein Ausdruck nicht ausreichend ist, sondern dass die Daten dem Kunden in maschinenlesbarer Form zur Verfügung gestellt werden müssen.

Auch diese Funktion kommt in einer der nächsten Versionen ab 2.0.346.

Löschkonzept

Das Löschen der personenbezogenen Daten steht an einigen Stellen im Widerspruch zu den gesetzlichen Aufbewahrungspflichten.

Für uns interpretieren wir aus den bestehenden und neuen Gesetzen und Verordnungen die folgende Vorgehensweise für das Löschen von Daten.

Belegdaten werden erst nach 10 Jahren gelöscht

Alle belegbezogenen Daten in der Warenwirtschaft die aus der Auftragsbearbeitung, dem Bestellwesen, der Kasse und der Lagerwirtschaft kommen, werden mindestens 10 Jahre in der Datenbank aufbewahrt.

Frühere Einstellungen im ControlCenter zur Löschung von Belegen werden damit ab der Version 346 unwirksam.

Sollten Sie bei Verwendung des kostenlosen Microsoft Express SQL-Servers Probleme mit der maximalen Datenbankgröße von 10GB bekommen, haben Sie 2 Möglichkeiten:
1. Sie kaufen die Originalversion des SQL Servers von Microsoft
2. Sie erstellen mit Hilfe unseres Supports eine Sicherungs-Kopie der aktuellen Datenbank und löschen dann aus der aktuellen Datenbank die ersten Jahre um wieder Platz zu schaffen. Bei Bedarf (Prüfung) muss dann die Datenbank-Kopie wieder installiert (z.B. als Mandant 1) werden, um die Daten einzusehen und ggfs. zu exportieren. Unser Support hilft Ihnen dann auch bei der Bereinigung der aktuellen Datenbank.

Stammdaten löschen

Alle Stammdaten, bei denen das Löschkennzeichen auf ´zur Löschung vorgesehen´ gesetzt wurde, werden in einem Löschlauf, der jede Nacht stattfindet, nach den folgenden Regeln gelöscht.

1. Ist der Datensatz nirgendwo mit einem aufbewahrungspflichtigen Beleg in der

Auftragsbearbeitung, Bestellwesen, Lagerhistorie oder der Kasse verknüpft, wird er komplett restlos und unwiederbringlich aus der Datenbank entfernt.

2. Ist der Datensatz an irgend einer Stelle mit Belegdaten verknüpft sind, wird dieser nicht physisch aus der Datenbank gelöscht, sondern nur mit einem Löschkennzeichen ´GELÖSCHT!´ versehen. Datensätze mit diesem Kennzeichen werden dann in den folgenden Versionen in Suchergebnissen, Reports und Grids ausgeblendet.

3. Handelt es sich bei diesem Datensatz um den Stammsatz eines Endverbrauchers, wird der gesamte Datensatz restlos und unwiederbringlich geleert. In den Namen wird das Kennzeichen 'xxxxx GELÖSCHT xxxxx' geschrieben.

Damit wird sichergestellt sein, dass diese Daten im laufenden Betrieb nicht mehr verwendet werden können. Gleichzeitig bleibt aber die Integrität der Datenbank erhalten, was für Listen, Auswertungen und auch für Exporte z.B. bei Betriebsprüfungen unabdingbar ist.

Abweichend davon bleiben aber auch die von Privatkunden erfaßten Adressdaten in der Auftragsdatenbank erhalten. Denn hier widerspricht eine tatsächliche Löschung unserer Meinung nach den Gesetzen der Aufbewahrungspflichten. Hier werden die Daten erst nach Ablauf der gesetzlichen Aufbewahrungspflicht gelöscht.

Sollte sich das auf Grund von neuen Regelungen, Klärungen oder Urteilen in den nächsten Jahren ändern, passen wir das selbstverständlich diesen neuen Regelungen an.

Wir können uns z.B. vorstellen, dass wir durch Parameter gesteuert die Löschung eines Privatkunden auch auf die Auftragsdatenbank ausweiten und auch dort die gespeicherten Kundendaten physisch löschen, wenn Sie z.B. durch ein Dokumentenmanagementsystem (DMS) Ihren Aufbewahrungspflichten nachkommen können.

Im Rahmen unseres Programms ist aber auf jeden Fall sichergestellt, dass diese Daten nur die Anwender mit den entsprechenden Rechten (Auftragsbearbeitung) einsehen dürfen.

Auch hier werden wir in den nächsten Versionen die Kontrolle auf das Datenschutzkennzeichen im Benutzerstamm mit in Betracht ziehen.

Eine weitere Verwendung der in den Belegen erfassten Anschriften ist nicht im Rahmen des Programms vorgesehen und auch nicht erlaubt.

Wir empfehlen Ihnen aber, besonders diesen Punkt bei der Erstellung Ihrer eigenen Verfahrensanweisung und Ihres Löschkonzeptes mit Ihrem Berater noch einmal zu besprechen. Sollten Sie hier individuelle Wünsche haben, sprechen Sie uns bitte an.

Vertrag zur Auftragsdatenverarbeitung (ADV) mit unseren Kunden?

Eigentlich müssten wir mit unseren Kunden einen rechtsverbindlichen Vertrag zur ADV schließen, da wir per Fernwartung ja theoretisch Ihre (Endkunden) Daten einsehen und downloaden könnten.

Wenn man aber den Gesetzestext genau liest, gibt es eine Ausnahme:

„Aufträge über Wartung oder Prüfung von IT-Systemen stellen keine Auftragsverarbeitung dar, sofern Gegenstand des Vertrages keine Datenverarbeitung ist, sondern allein auf die Supportleistung abzielt.“ Nach DSGVO müsste deswegen kein ADV-Vertrag geschlossen werden. „Vielmehr müssen Wartung und Prüfung so organisiert und geregelt werden, dass die Daten entsprechend den in Art.24 DSGVO festgelegten Pflichten des Verantwortlichen angemessen geschützt sind.“

Auch bei uns besteht unsere Vertragsbeziehung in Bezug auf den Teleservice nur in den wesentlichen Aufgaben, die im Mietvertrag und den AGB geregelt sind:

- Pflege von unserer WWS-Software und dazu gehörigen Anwendungen
- Fehlersuche und Tests

Deshalb reicht es, wenn wir Ihnen an dieser Stelle versichern, dass unsere Mitarbeiter entsprechend geschult wurden und schon immer in separaten Vereinbarungen zu deren Anstellungsverträgen zur absoluten Verschwiegenheit und Datenschutz verpflichtet wurden.

Wir werden Ihre (Endkunden)Daten nicht einsehen oder gar herunterladen, es sei denn, das ist zum Zwecke der Fehlerrecherche unabdingbar. In diesem Fall werden wir Ihre komplette Datenbank laden und sofort nach dem Erkennen der Fehlerursache restlos und unwiederbringlich löschen. Download, Recherche und Löschung erfolgen in diesen – sehr seltenen Ausnahmefällen – immer innerhalb eines Arbeitstages.

Unsere Empfehlungen für Sie

Sie sollten unverzüglich, (optimalerweise unter Hinzuziehung ihres Rechtsberaters oder eines Datenschutz-Dienstleisters) mit der Umsetzung beginnen!

Klären Sie (mit dem Berater) u.a. folgende Fragen:

+ Wie klären Sie Ihre Kunden über die Aufbewahrung und Verwendung der personenbezogenen Daten auf?
+ Erstellen Sie ein für Sie gültiges Löschkonzept, gerne mit Verwendung dieser Dokumentation
+ Geben Sie Ihren Kunden die Möglichkeit, sich von Newslettern und Rundschreiben auszuschließen (Opt-In).
+ Haben Sie einen Datenschutzbeauftragten (notwendig?)?
  Wenn ja, benennen und schulen Sie diesen.
+ Brauchen Sie das Datenverarbeitungsverzeichnis?
+ Erfordert die DSGVO eine Verschlüsselung oder Pseudonymisierung der Daten in Ihrem konkreten Anwendungsfall? Dann kontaktieren Sie uns bitte, damit wir Ihnen konkrete Angebote machen können.
+ Gewähren Sie entsprechende Rechte, wie z.B. Recht auf Vergessen, Recht auf Datenübertragbarkeit usw.
+ Bereiten Sie sich auf mögliche Datenverluste vor: Führen Sie Eskalationsverfahren ein, die im Falle eines Verstoßes gegen personenbezogene Daten eingeleitet werden.

Das Thema ist wichtig und darf auch keinen Fall unterschätzt oder vernachlässigt werden! Es drohen hohe Bußgelder und auch die Abmahngefahr durch Wettbewerber ist nicht zu unterschätzen.

Holen Sie sich bitte professionelle Hilfe, wenn Sie oder Ihr Datenschutzbeauftragter die Anforderungen nicht erfüllen können. Es besteht auf jeden Fall Investitionsbedarf.