# Bewertung: Datenschutz durch Technikgestaltung[[1]](#footnote-1) („by Design“) und durch datenschutzfreundliche Voreinstellungen („by Default“)

|  |  |
| --- | --- |
| **Übersicht** |  |
| |  |  |  |  | | --- | --- | --- | --- | | Kennung | 5010 - dPerso | Datum | 24.06.2019 |   **Eingliederung** dieses Dokuments in die **Gesamtdokumentation**   |  |  |  | | --- | --- | --- | | Diese Bewertung (Überlegungen und Entscheidungen) zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen ist **folgendem Dokumentationsbestandteil** (Dokumentation eines Systems, einer Software, eines Netzes, einer Verarbeitungstätigkeit usw.) zugeordnet: *(eine Mehrfachauswahl ist möglich)* | | | |  | Technisches/nichttechnisches System | Name des Systems eingeben | |  | Software | dPersonalmanagement (dPerso) | |  | Netze | Name des Netzwerks/Netzgerätes eingeben | |  | Verarbeitungstätigkeit | Bezügeabrechnung der Beschäftigten mit dPerso | |  | Infrastruktur | Name des Infrastrukturelements (materielle oder immaterielle Grundausstattung) eingeben | |  | Sonstiger Dokumentations­bestandteil | Name des sonstigen Dokumentationsbestandteils eingeben |  |  |  | | --- | --- | | Speicherort der **internen Strategien zur Umsetzung des Art. 25 DSGVO** *(Verweis auf das übergeordnetes Dokument, dass die internen Strategien festlegt, die insbesondere den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen Genüge tun (EWG 78 DSGVO) )* | | |  | Bislang ist ein internes Strategiepapier zur Umsetzung des Art. 25 DS-GVO noch nicht erstellt worden, die DSB stellt Fragen nach der Protokollierung, dem Rollen-Rechte-Konzept, dem Löschkonzept und der Verschlüsselung.  Das Strategiepapier soll bis zum 01.07.2020 erstellt werden. |  |  |  |  | | --- | --- | --- | | Weitere **übergeordnete** (üD) oder **untergeordnete** (uD) Dokumente  *(falls über- oder untergeordnete Dokumente vorhanden sind, dann können sie hier aufgeführt werden)* | | | |  | üD | ggf. Name und Speicherort der übergeordneten Dokumente aufführen | |  | uD | ggf. Name und Speicherort der untergeordneten Dokumente aufführen | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | |  | (1) Datenschutz durch **Gestaltung** des Verarbeitungssystemsund durch **datenschutzfreundliche** **Voreinstellungen** zum **Zeitpunkt** der **Ausschreibung und Auswahl des Verarbeitungssystems** |  |  |  |  |  | | --- | --- | --- | --- | | Wurden die Datenschutzgrundsätze mit Hilfe der **Technikgestaltung** und datenschutzfreundlicher **Voreinstellungen** bei **der Ausschreibung** und **Auswahl des Verarbeitungssystems** berücksichtigt? |  |  | | | *Bei* ***ja:*** *Die berücksichtigten Maßnahmen unter* ***1.1*** *dokumentieren und bewerten.*  *Bei* ***nein:*** *Die fehlende Berücksichtigung unter* ***1.2*** *begründen.* | | |  |  |  | | --- | --- | | (1.1) **Dokumentation** und **Bewertung** der berücksichtigten **Maßnahmen** zur **datenschutzkonformen** **Technikgestaltung** und **datenschutzfreundlichen Voreinstellungen** im Ausschreibungs- und Auswahlprozess  Betrachtete Komponente: 1: Hardware 2: Software 3: Netze  4: Prozesse 5: Anweisungen 6: Organisation  7: Sonstige Komponente | | | Komponente | Bemerkungen | |  |  |  |  | | --- | | (1.2) Für den Fall, dass ein oder mehrere Datenschutzgrundsätze nicht berücksichtigt wurden, Begründung   * **der fehlenden** Berücksichtigung bei der **Gestaltung** * **der fehlenden** Berücksichtigung bezüglich **datenschutzfreundlicher** Voreinstellungen   zum **Zeitpunkt** der **Ausschreibung** und **Auswahl** des Verarbeitungssystems | | Vor dem Start des Verfahrens dPerso (damals unter dem Namen KoPers kommunal) zum 1.1.2014 hat sich eine Arbeitsgruppe länderübergreifend mit einem Nachfolgeverfahren für Permis A beschäftigt. Zu diesem Zeitpunkt gab es die Vorgaben der DS-GVO noch nicht. | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | |  | (2)Datenschutz durch **Gestaltung** zum **Zeitpunkt** der **Verarbeitung** |  |  |  |  | | --- | --- | --- | | Werden die Datenschutzgrundsätze sowie die Anforderungen der DSGVO durch **technische und organisatorische Maßnahmen** zum Zeitpunkt der Verarbeitung gewährleistet? |  |  | | *Bei* ***ja:*** *Die getroffenen Maßnahmen unter* ***2.1*** *dokumentieren und bewerten.*  *Bei* ***nein:*** *Die fehlende Berücksichtigung unter* ***2.2*** *begründen.* | | |  |  |  | | --- | --- | | (2.1) **Dokumentation** und **Bewertung** der getroffenen **technischen** und **organisatorischen** Maßnahmen **zu Datenschutz durch Gestaltung des Verarbeitungssystems**  Betrachtete Komponente: 1: Hardware 2: Software 3: Netze  4: Prozesse 5: Anweisungen 6: Organisation  7: Sonstige Komponente | | | Komponente | Bemerkungen | | 2 | * VPN Zugang * IP basierte Zugangsbeschränkung * eindeutiger Anmeldename und Passwort * Verschlüsselung von Datenträgern * regelmäßige Softwareupdates * regelmäßige Auswertung von Server-Protokollen * Protokollierung von Aktivitäten * Rechte und Rollen (lesen, schreiben, ändern, löschen) * anonymisierte Daten bei Entwicklungs- und Testsystemen * logische Datentrennung   (siehe auch CD) |  |  | | --- | | (2.2) Begründung bei einer   * **fehlenden** **Gestaltung** des Verarbeitungssystems durch technische und organisatorische Maßnahmen   zum **Zeitpunkt der Verarbeitung** | | Hier die fehlende Berücksichtigung begründen | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | |  | (3) Datenschutz durch **datenschutzfreundliche** **Voreinstellungen** |  |  |  |  | | --- | --- | --- | | Wurden **datenschutzfreundliche Voreinstellungen** geplant und konfiguriert, um nur diejenigen personenbezogenen Daten zu verarbeiten, deren Verarbeitung für den jeweiligen Verarbeitungszweck erforderlich sind? |  |  | | *Bei* ***ja:*** *Die Voreinstellungen unter* ***3.1*** *dokumentieren und bewerten.*  *Bei* ***nein:*** *Die fehlende Umsetzung unter* ***3.2*** *begründen.* | | |  |  |  | | --- | --- | | (3.1) **Dokumentation** und **Bewertung** der getroffenen **Maßnahmen** zu **datenschutzfreundlichen** **Voreinstellungen**  Mögliche Komponenten: 1: Hardware 2: Software 3: Netze  4: Sonstige Komponente | | | Komponente | Bemerkungen | | 2 | * Vorkonfiguration von verschiedenen Rollen * Verschlüsselung der Daten * Protokollierung derAktionen * Abprüfung IP Adresse und 2 Faktor Authentifizierung |  |  | | --- | | (3.2) Begründung bei einer   * **fehlenden Berücksichtigung** von **datenschutzfreundlichen** **Voreinstellungen** | | Hier die fehlende Berücksichtigung begründen | |

1. In der englischen DSGVO heißt es „Data protection by design“; insbesondere soll sich der Fokus auf die gesamte Gestaltung der Verarbeitungssysteme (d. h. Hardware, Software, nichttechnische Systeme (z. B. Akten), organisatorische Maßnahmen) beziehen, anstatt nur die Technik in den Blick zu nehmen. [↑](#footnote-ref-1)