Datenschutz

DSGVO-Konformität erreichen

[09.07.2021] Auf ihrem Weg zur DSGVO-Konformität sollten Verwaltungen kooperativ, agil und modular vorangehen. Das Thema Datenschutz muss transparent und für alle nachvollziehbar gestaltet werden.

Datenschutz muss Teil der Arbeitsorganisation in Verwaltungen werden. Das hat der erste Teil dieses Beitrags gezeigt. Im Folgenden werden nun Schritte aufgezeigt, die zur Herstellung der DSGVO-Konformität einer Verwaltung beitragen. Sie sollten unter Berücksichtigung der Integration in die Arbeitsorganisation durchgeführt werden. Sowohl die Schrittfolge als auch die einzelnen zu prüfenden Sachverhalte innerhalb der Schritte sind in Bausteine zerlegt, sodass Individualisierung und Standardisierung gleichermaßen erreicht wird.
Zunächst muss unbedingt organisationsweit ermittelt werden, bei welchen Geschäftsprozessen – seien es Fach- oder Querschnittsprozesse – in welcher Art personenbezogene Daten verarbeitet werden. Dazu müssen der Datenschutzbeauftragte (DSB), IT-Experten, die Fachebene und gegebenenfalls weitere Beauftragte intensiv kommunizieren. Diese kollaborativen Prozesse sind methodisch zu unterstützen.

Für alle verständlich

Die Datenschutzthematik muss für alle Bereiche einer Organisation vereinfacht, verständlich und nachvollziehbar gestaltet werden. Hierfür lassen sich entsprechende Bausteine definieren. Das können etwa der Zweck der Datenerhebung, die Verarbeitungsart der Daten oder der Zugang zu Daten sein. Abgeleitet werden sie aus den fachlichen Anforderungen der DSGVO und folgen einer vordefinierten Systematik. Die Bausteine sind so aufgebaut, dass nur das erhoben werden kann, was tatsächlich relevant und erforderlich ist. Mittels einfacher haptischer Karten und einer entsprechenden Moderation können auch Nichtexperten durch den DSGVO-Prüfprozess geleitet werden. Dabei werden die Datenschutzanalysen entlang von Fachprozessen vollzogen, um so eine enge Rückkopplung zur Arbeitsebene herzustellen und diese im Weiteren mit IT-Fragen zu verknüpfen. Durch dieses Vorgehen findet bereits bei der Datenerhebung eine fachübergreifende Zusammenarbeit und ein entsprechender Austausch der jeweiligen Experten (IT, Recht, Organisation, Management) statt. Es handelt sich also nicht mehr nur um eine bloße Informationssammlung. Es werden bereits Umsetzungs- und Gestaltungsfragen thematisiert.

Intuitives Lernen und Risikobewertung

Aus der Lernforschung ist bekannt, dass es trotz oder gerade wegen der zunehmenden Digitalisierung wichtig für das menschliche Verstehen ist, physisch greifbare Bestandteile zu haben. Komplexe Sachverhalte erscheinen den Mitarbeitenden dann nicht mehr abstrakt, sondern verständlich, nachvollziehbar und letztlich anfassbar. Durch die Haptik wird ein intuitives Lernen ermöglicht. So wird im hohen Maße eine Beteiligung/Mitwirkung erreicht, was die Akzeptanz für das Thema Datenschutz sowie die Akzeptanz in der späteren Umsetzung deutlich erhöht. Lernen und Arbeiten gehen zunehmend ineinander über und lassen sich in einer solchen Methodenwelt nicht mehr trennen. Digitalisierung kann dabei das kollaborative Arbeiten auf Entfernung unterstützen. Automatisierungspotenzial besteht dahingehend, dass die erhobenen Daten automatisch grafisch aufbereitet und auf Vollständigkeit sowie Plausibilität geprüft werden, um Erhebungslücken aufzuzeigen.

Ein nächster wichtiger Schritt ist die Risikobewertung. Es muss eingeschätzt werden, welches Risiko für Schutzverletzungen bei der Verarbeitung personenbezogener Daten besteht. Hier können grundsätzlich Algorithmen – auch analog umgesetzt – unterstützen, indem beispielsweise auf Basis eines organisationseigenen Kriteriensets Empfehlungen zur Interpretation der erhobenen Informationen und bei der Zuordnung zu Risikoklassen gegeben werden. Weiterhin lassen sich Folgen von Entscheidungsalternativen aufzeigen. Eine Datenschutzfolgenabschätzung könnte zum Beispiel nötig sein, wenn eine bestimmte Risikoklasse gewählt wurde. Als Grundlage für solche Empfehlungen können generische Kriterien genutzt werden, die unter anderem auf den Empfehlungen des Standarddatenschutzmodells (SDM V2.0) der DSK basieren. Insgesamt lässt die DSGVO an dieser Stelle aber sehr viel Interpretationsspielraum, sodass die Letztentscheidung bei den jeweiligen Verantwortungsträgern liegen muss.

Technische und organisatorische Schutzmaßnahmen

Sind die Risiken definiert, sind geeignete technische und organisatorische Schutzmaßnahmen (TOM) zu bestimmen. Die Entscheidung darüber, welche Maßnahmen geeignet sind, setzt vertiefte Organisations- und IT-Kenntnisse im Zusammenspiel voraus. Empfohlen wird der Einbezug von IT- oder IT-Sicherheitsexperten. Sie wissen, welche TOM sich für welche Datenschutzsituation eignen. Vorgeschlagen wird, die Maßnahmen auf der Basis des organisationseigenen Katalogs zu diskutieren, um Synergien bei der Umsetzung erzielen zu können und damit Ressourcen zu sparen. Eine weitere Basis könnte der generische Katalog des Standarddatenschutzmodells der DSK sein. In dieser Diskussion entscheiden alle Beteiligten gemeinsam, welche Maßnahmen als obligatorisch für die DSGVO-Konformität empfohlen werden und welche als fakultativ.
Wurde entschieden, welche TOM erforderlich sind, muss überprüft und abgeglichen werden, welche TOM noch umzusetzen und welche bereits umgesetzt sind oder welcher Umsetzungsgrad bereits erreicht ist. Auf Basis dieser Angaben kann ein Soll-Ist-Abgleich erfolgen, um den Konformitätsgrad zu ermitteln. Auf Basis individuell festgelegter Kriterien kann eine Priorisierung der Umsetzung in Bezug auf fehlende Schutzmaßnahmen erfolgen, um den Konformitätsgrad möglichst schnell zu erhöhen. Dies ist eine strategisch angeleitete Vorgehensweise, bei der Datenschutz nicht nach dem Gießkannenprinzip praktiziert wird, sondern gezielt Ressourcen eingesetzt werden, wo es tatsächlich notwendig ist.

Automatische Dokumentation

Die Tätigkeit des DSB ist sehr stark geprägt von der Erstellung von Nachweisen für die Konformität, wie sie nach der DSGVO gefordert sind (Verarbeitungsverzeichnis). Hierbei sollte ihn möglichst ein IT-Tool unterstützen. So ein Tool erstellt auf Basis der qualitativ hochwertigen Daten automatisch die geforderten Berichte in gebotener Qualität. Um den Aufwand für den DSB und Verantwortliche so gering wie möglich zu halten, müssen die Dokumente adressatengerecht, also beispielsweise für Aufsichtsbehörden oder für Betroffene passend gestaltet sein. Für den DSB hat das vorher beschriebene Vorgehen den Vorteil, dass er nicht aufwendig und separat ein Verarbeitungsverzeichnis erstellen muss. Vielmehr ergibt sich durch die prozessnahen Erhebungen datenschutzrelevanter Aspekte nebenbei das von der DSGVO geforderte Verzeichnis aller Verarbeitungstätigkeiten inklusive entsprechender Prozessdarstellungen, Risikobewertungen und Dokumentation der technisch-organisatorischen Maßnahmen. Damit reduziert sich der Aufwand für Datenschutzbeauftragte erheblich. Führungskräfte und Behördenleitung, die Datenschutzverantwortliche nach der DSGVO sind, erhalten somit auf einfache Weise eine Dokumentation und bekommen die Komplexität und Vielfältigkeit des Themas besser in den Griff.

Mit PRIMO transparent und nachvollziehbar

Letztendlich funktioniert die DSGVO als Compliance-Anforderung nur dann, wenn sich Organisationsroutinen und -kulturen ändern und Anforderungen in der Breite der Organisation als Routine mit dauerhaften Verhaltensänderungen niederschlagen. Vernünftig gestaltete und akzeptierte Methoden können wesentlich dabei helfen, sich in neue Routinen hineinzubewegen. Fachübergreifende Kooperation wird gefördert, sodass Raum für Lernprozesse entsteht. Dafür muss die Komplexität des Themas Datenschutz durch intelligente Tools reduziert werden, um die Anwendung von Datenschutz für die Organisation handhabbar zu gestalten. Das im Artikel beschriebene Vorgehen ermöglicht genau das. Um die praktische Umsetzung zu erleichtern, hat das SHI Stein-Hardenberg Institut, in Zusammenarbeit mit eGovCD – einem SpinOff des Fraunhofer-Instituts für Offene Kommunikationssysteme FOKUS – dieses methodisch strukturierte und modulare Vorgehen in das Tool PRIMO gegossen. Durch eine datenschutzsensible Prozessgestaltung werden Mitarbeitende dort abgeholt, wo personenbezogene Daten in den Arbeitsprozessen verarbeitet werden. Für jeden Prozess wird gemeinsam ein einheitliches Verständnis geschaffen, sodass Datenschutz nicht getrennt von anderen Bereichen betrachtet oder an Experten wegdelegiert wird. Das hat den großen Vorteil, dass das Thema aus der juristischen Fachecke herausgeholt und die Komplexität reduziert wird, sodass im Ergebnis eine datenschutzkonforme Prozessgestaltung stattfindet. Im Rahmen agiler Vorgehensweisen lässt sich das methodische Vorgehen hervorragend einsetzen, ohne dabei allzu tiefes Datenschutzwissen haben zu müssen. Damit ist PRIMO sowohl ein Tool zur Umsetzung von Datenschutzanforderungen als auch ein Sensibilisierungswerkzeug, das das Lernen in der Organisation untereinander unterstützt.

()

Weitere Informationen zum Tool PRIMO

Stichwörter: Politik, Datenschutz