title Der Standard
issue 26/03/2018
page 12

Höchste Zeit für den Datenschutznotfallplan

Bei der Vorbereitung zum DSGVO-Start müssen Prioritäten richtig gesetzt werden

Axel Anderl

Wien – Die Stunde null der Datenschutz-Grundverordnung (DSGVO) am 25. Mai naht schnell, und bis dahin ist für Unternehmen noch viel zu tun. Umso wichtiger ist ein zielgerichteter Notfallplan, mit dem die verbleibende Zeit durch klare Prioritätensetzung bestmöglich genutzt wird.

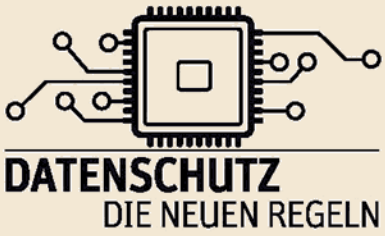
Zu Beginn sollten strukturelle Fragen stehen: Wer ist intern für die Umsetzung zuständig (Recht, Technik, Geschäftsführung)? Wie hoch ist das interne und externe Budget, sind externe Berater notwendig und noch verfügbar? Dann sollte vorab geklärt werden, ob im Unternehmen ein Datenschutzbeauftragter erforderlich ist – und die Entscheidung dokumentiert werden. Wenn ja, sollte die Position rasch besetzt werden, damit er von Anfang an in die Umsetzung eingebunden ist.

Inhaltlich muss das bestellte Projektteam prüfen, welche Verarbeitungen im Unternehmen

- wegen Profiling, strafrechtlich relevanter Daten oder systematischer Überwachungen ein voraussichtlich hohes Risiko für die Betroffenen begründen;
- sensible Daten (Gesundheit, sexuelle Orientierung, religiöse Anschauungen, rassische oder ethnische Herkunft) betreffen; oder
- durch ihre Masse oder Relevanz geschäftskritisch sind.

In diesen Fällen ist eine umfängliche Erhebung und Analyse des Zwecks, der Rechtsgrundlage und Verhältnismäßigkeit durchzuführen. Auf dieser Basis ist dann das vollständige Verfahrensverzeichnis zu erstellen, die Datenschutzfolgeabschätzung durchzuführen sowie Löschfristen und allfällige technische Sicherheitsmaßnahmen zu implementieren.

Als nächster Schritt sind die Zustimmungserklärungen – sei es auf der Website, in den Kundenverträgen oder von Mitarbeitern – zu überarbeiten. Dabei ist auch der formale Aspekt der Entkoppelung zu berücksichtigen: Die Vertragserfüllung darf nicht an die Zustimmung zu für den Vertragsabschluss nicht erforderlichen Datenverarbeitungen gebunden werden. Erfahrungsgemäß besteht hier ein großer Abstimmungsbedarf mit der Marketingabteilung. Es empfiehlt sich, auch die oft noch immer nicht gesetzeskonformen Direktwerbemaßnahmen (Spamverbot nach § 107 TKG) zu überprüfen.



Ebenso wichtig ist es, die bisherigen Dienstleistervereinbarungen durch DSGVO-konforme Auftragsverarbeitungsvereinbarungen zu ersetzen. Auch für die neuen, umfangreichen Informationspflichten gegenüber Betroffenen und Abläufe zur Sicherstellung der Durchsetzung ihrer schon jetzt sprunghaft stärker ausgeübten Rechte sind Vorkehrungen zu treffen. Die dafür notwendigen Prozesse haben daher absolute Priorität.

Für nicht priorisierte Datenverarbeitungen sind zumindest auf Basis der bisherigen DVR-Meldungen ein provisorisches Verarbeitungsverzeichnis sowie die Datenschutzhinweise zu erstellen; all das zur Haftungsvermeidung jedenfalls vor dem 25. Mai.

Mustermeldung vorbereiten

Sobald die Kernaufgaben erfüllt sind, gilt es die provisorischen Verzeichnisse mit der Realität im Unternehmen abzugleichen, die nach der DSGVO erforderlichen Zusatzinformationen zu ergänzen sowie etwaig notwendige Folgeabschätzungen nachzuziehen. Weiters sollte man allgemeine Datensicherheitsmaßnahmen setzen, interne Policies verabschieden und Mitarbeiter schulen. Zuletzt ist eine Mustermeldung für etwaige Datenschutzvorfälle vorzubereiten, damit man im Ernstfall für die knappe 72-Stunden-Meldefrist gewappnet ist.

All diese Maßnahmen müssten eigentlich schon zum 25. 5. umgesetzt sein. Jene nicht priorisierten Themen, die sich nicht zeitgerecht oder vollumfänglich ausgegangen sind, sind daher möglichst rasch nachzuholen, um zu verhindern, dass aus dem Provisorium ein rechtlich unzulässiges Fixum wird, das Haftungen verursachen kann.

AXEL ANDERL ist Managing Partner bei Dorda Rechtsanwälte, leitet das IT/IP-Team und ist Co-Leiter der Datenschutzgruppe. axel.anderl@dorda.at