Mit dem Datenschutz gilt es nun ernst

Von Dr. iur. Monika Pfaffinger
Head of Data Protection
and Privacy Practice
Lexperience AG
Legal & Compliance Services

und lic. iur. Nadine Balkanyi-Nordmann
Rechtsanwältin, LL.M., FCIArb.
CEO
Lexperience AG
Legal & Compliance Services

In den Tagen vor dem 25. Mai 2018, dem Datum, an dem die Frist zur Umsetzung der Europäischen Datenschutzgrundverordnung (DSGVO/GDPR) ablief, häuften sich auch bei den schweizerischen Beratungsunternehmen mit Datenschutzexpertise verzweifelte Anfragen: «Könntet ihr uns bitte compliant mit der DSGVO machen?»

Also machte man sich an die Arbeit. Denn: Mit der Datenschutz-Compliance und Datensicherheit gilt es nun ernst. Während sich die erste Panik im Lauf des Hitzesommers legte, folgte am 10. Oktober 2018 vom EU-Datenschutzbeauftragten Buttarelli die Ankündigung, dass Unternehmen bis Jahresende mit den ersten Sanktionen und Massnahmen bei Verletzungen der verschärften datenschutzrechtlichen Vorgaben gemäss der DSGVO zu rechnen hätten. Die zuständigen nationalen Datenschutzbehörden würden, so der EU-Datenschutzbeauftragte, mit Anfragen und Beschwerden überflutet. Wenn der EU-Datenschutzbeauftragte ankündigt, dass in Bälde mit Strafen, Rügen, Ultimaten und vorübergehenden Firmenverboten zu rechnen sei, wird damit deutlich, dass der Massnahmenkatalog gemäss DSGVO weit- und tiefgreifend ist. Er geht markant über die mit Indignation thematisierten hohen Bussen bei Verstössen gegen die DSGVO hinaus.

Die Fokussierung auf die entsprechenden Bussen, aber auch die facettenreichen behördlichen Massnahmen, vermögen allerdings nicht abzubilden, wie grundlegend die Neuerungen sind, die mit der DSGVO einhergehen. Es ist nicht übertrieben, von einem *Paradigmenwechsel* im Datenschutzrecht zu sprechen, der von der DSGVO angestossen wird. Die starke Hand der Datenschutzbehörden auf der Stufe der Rechtsdurchsetzung ist nur *ein* Element, der Ausbau der Betroffenenrechte, der Transparenz- und Einwilligungsvorgaben sind weitere Faktoren.

Anwendbarkeit der DSGVO auch für Schweizer Unternehmen

Die DSGVO harmonisiert das Datenschutzrecht im EU-Raum, was auch der Tatsache der «grenzenlosen» Verarbeitungskapazitäten der neuen Informationstechnologien geschuldet ist und dem Schutz des Menschen, aber auch der Prosperität und dem Fortschritt dienen soll. Die DSGVO hat einen «langen Arm»; aufgrund ihrer *extraterritorialen Wirkung* können entsprechend auch Schweizer Unternehmen in ihren Anwendungsbereich fallen. Das allerdings wurde hierzulande bislang nur von einem Teil der Verantwortlichen zur Kenntnis genommen. Daher nochmals: Mit Blick auf den räumlichen Anwendungsbereich ist vorab das Niederlassungsprinzip einschlägig, Art. 3 Abs. 1 DSGVO. Sodann fällt man in den Anwendungsbereich der DSGVO aufgrund des sog. Angebotstatbestandes gemäss Art. 3 Abs. 2 lit. a DSGVO, sofern man Waren oder Dienstleistungen betroffenen natürlichen Personen in der EU anbietet. Zudem ist die DSGVO einschlägig gemäss des sog. Tracking-Tatbestandes, falls man das Verhalten von betroffenen Personen in der EU beobachtet, Art. 3 Abs. 2 lit. b DSGVO. Für viele Schweizer Unternehmen ist entsprechend an erster Stelle eine *Basisanalyse* angezeigt, ob und inwiefern man mit seinen Personendatenverarbeitungen *im Scope der DSGVO* ist oder nicht. Mit einer sorgfältigen Prüfung der Frage des Anwendungsbereichs wird zugleich dem Accountability-Ansatz der DSGVO Rechnung getragen.

Neue Verantwortlichkeiten zur faktischen Verwirklichung

Der *Accountability-Ansatz* auferlegt den Verantwortlichen umfassende Dokumentations- und Rechenschaftspflichten betreffend der getroffenen Massnahmen zur Einhaltung der Datenschutz-Compliance und -Sicherheit. Mit diesem Ansatz wird ein Perspektivenwechsel vollzogen, indem nunmehr – anders als in einem isoliert persönlichkeitsrechtlich und damit

deliktsrechtlich, abwehrrechtlich gedachten Datenschutzrecht – *personendatenverarbeitende Stellen früher und nachhaltig in die Pflicht* genommen werden. Ebendies wird auch mit der neuen Bezeichnung der Personendatenverarbeitenden als «Verantwortliche» ausgedrückt. Mit dem Ansatz setzt man an einem Kerndefizit des bisherigen Datenschutzrechts an: der ungenügenden faktischen Einhaltung durch die Verarbeitenden. Auch für die Schweiz wurde evaluiert, dass die Vorgaben des geltenden Datenschutzgesetzes «lasch» gehandhabt wurden und werden – nicht zuletzt, weil man bei Verstössen kaum je mit Konsequenzen zu rechnen hatte. Allerdings liess sich in den letzten Jahren eine Intensivierung der Interventionen von Seiten des EDÖB verzeichnen. Zudem zielen zahlreiche weitere und neue Instrumente der DSGVO, aber auch der geplanten Totalrevision des eidgenössischen Datenschutzgesetzes (DSG) ihrerseits darauf ab, das Datenschutzrecht in der Praxis griffig zu machen.

Akuter Handlungsbedarf in komplexem Regelungsregime

Zur *Totalrevision des DSG* sind die parlamentarischen Beratungen angelaufen, mit dem Inkrafttreten wird allerdings nicht vor 2020 gerechnet. Ziel der Revision ist eine Annäherung an die DSGVO. Damit ist auch gesagt, dass Differenzen im Schutzniveau bleiben werden. Indem indes die Datenschutzvorgaben mit der Revision gleichwohl angehoben werden und das noch geltende Datenschutzrecht bislang sportlich gehandhabt wurde, ist für viele Schweizer Unternehmen der *Nachhol- und Handlungsbedarf* heute beträchtlich und akut. Einige Schweizer Unternehmen sehen sich hierbei mit einem verzahnten Regelungsregime konfrontiert, indem für sie nicht nur die DSGVO, sondern auch das DSG sowie sektorspezifische Erlasse einschlägig sein können. Exemplarisch hierzu ist der Bankensektor mit dem Bankengesetz und dem Finma-Rundschreiben über operationelle Risiken, das den Datenschutz beinhaltet.

Aufbau der Datenschutz-Compliance

Die Herausforderung, die Datenschutz-Compliance zu gewährleisten, wird folglich auch Unternehmen in der Schweiz in den kommenden Jahren intensiv beschäftigen. Denn so selbstverständlich heute Massnahmen zur Einhaltung des Geldwäschereigesetzes oder die Kartellrechts-Compliance sind, so selbstverständlich hat die Datenschutz-Compliance zu sein. Es ist Zeit, tragende Säulen jeder Datenschutz-Compliance aufzubauen. Sie umfasst namentlich technische, rechtliche und organisatorische Massnahmen. Ein Compliance-Framework geht entsprechend weit über das Weisungswesen hinaus und bedingt insbesondere die Etablierung von Prozessen, die Fixierung von Zuständigkeiten und Verantwortlichkeiten sowie die Durchführung von Kontrollen und Schulungen. Dass es bei der Umsetzung der Datenschutz-Compliance und -Sicherheit kein «one size fits all» gibt, lässt sich gut anhand des Themas Schulung illustrieren. Nicht nur, dass in jedem Unternehmen aufgrund des Geschäftsmodells spezifische Anforderungen zu berücksichtigen sind und Schulungen ebenso der Unternehmenskultur Rechnung tragen müssen; auch bei den Mitarbeitenden bestehen spezifische Anforderungen. Zwar müssen Basiswissen und -sensibilität bei allen Mitarbeitenden sichergestellt werden. Allerdings variieren die Anforderungen an Kenntnis und Bewusstsein, die mittels Weiterbildungen und Schulungen zu erreichen sind, von Organisationeinheit zu Organisationseinheit, von Position zu Position, beträchtlich. Entsprechend entwickeln viele der grossen Unternehmen ihre eigenen Schulungsprogramme.

Ein Kernelement für die Etablierung der Datenschutz-Compliance ist das *Verarbeitungsverzeichnis,* zu dessen Erstellung die DSGVO wie der Entwurf zur Totalrevision des DSG verpflichten. Die Inventarisierung der Personendatenverarbeitungsprozesse ist gewissermassen Herz wie Gehirn jeder Datenschutz-Compliance und Data-Governance. Als Grundlage auch der Gewährleistung des Accountability-Ansatzes liefert das Inventar zugleich ein Navigationssystem, um dem *risikobasierten Ansatz* der neuen Erlasse Rechnung zu tragen. Ebendieser findet sich in weiteren Instrumenten, wie der Verpflichtung zur Durchführung von Datenschutz-Folgenabschätzungen oder der Risikoanalyse im Rahmen des Datenschutzes durch Technikgestaltung. Dort, wo besondere Risiken identifiziert werden, beispielweise bei der Verarbeitung besonderer Datenkategorien oder bei spezifischen Verarbeitungshandlungen, sind die Anforderungen an die zu treffenden technischen, organisatorische, baulichen und rechtlichen Massnahmen höher. Entsprechend geht es um den Aufbau eines eigentlichen Risiko-Managements zur Gewährleistung des Datenschutzes und der Datensicherheit.

Der Weg zu einer neuen Datenkultur

Die Aufgabe, Unternehmen datenschutzkonform aufzustellen, ist komplex und bedingt zeitliche, finanzielle, und fachliche *Ressourcen*. Es gilt organisatorische Zuständigkeiten zu fixieren, für die verschiedenen Anforderungsfelder Massnahmenpakete zu definieren, diese risikobasiert zu priorisieren, organisatorisch zuzuweisen, umzusetzen und in der Folge zu überprüfen, nachzubessern und entsprechend der Entwicklungen zu aktualisieren. Im Sinne eines Erste-Hilfe-Plans sollten Schweizer Unternehmen zunächst auf EU-Töchter von Schweizer Müttern fokussieren. Hierbei empfiehlt es sich, von den EU-Behörden leicht überprüfbare Massnahmen vorgezogen zu implementieren, z.B. die Datenschutzerklärung für Webseitenbetreiber. Damit der datenschutzrechtliche Bedeutungswandel allerdings im Gesamten vollzogen wird, braucht es den «tone from the top», Verantwortlichkeiten bei den Linien und die Sensibilität der Mitarbeitenden. Die Idee, wonach die Datenschutz-Compliance im Alleingang durch einen internen Datenschutzbeauftragten gewährleistet wird, greift zu kurz. Den Datenschutz in die DNA des Unternehmens zu integrieren, bedingt und bedeutet, einen eigentlichen Kulturwandel zu vollziehen. Dass man der Datenschutzregulierung und ihrer Einhaltung Nachdruck verleiht, erstaunt für eine Gesellschaft, die sich selbst als Informationsgesellschaft und Personendaten als Gold bezeichnet, nicht. Die Aufgabe, mit Personendaten rechtmässig und verantwortungsvoll umzugehen, sollte keineswegs bloss als Traktieren von Seiten der Gesetzgeber verstanden werden. Vielmehr bietet sie die wertvolle Chance zum bewussten Umgang mit Personendaten.

pfaffinger@lexp.ch
balkanyi@lexp.ch
www.lexp.ch