UIMC

Von der DSGVO lernen:

Das revidierte Datenschutzgesetz pragmatisch umsetzen!

- schnelle Durchführung
- praxisnahe Lösungen
- sichere Umsetzung
- flexible Betreuung

Datenschutz
Informationssicherheit
Organisation / Strategie

UIMC | pragmatisch.erfahren.verständlich.

Besser UIMC fragen.

pragmatisch.erfahren.verständlich.

Von der DSGVO lernen heißt, das Rad nicht neu erfinden zu müssen

In den Jahren 2016 bis 2018 ging es in den Ländern der Europäischen Union ziemlich turbulent zu: Es herrschte große Verunsicherung hinsichtlich der Datenschutzgrundverordnung (DSGVO). Wie müssen verschiedene Vorgaben interpretiert werden? Wie sollen die neuen Vorgaben umgesetzt werden? Wie sollen wir das alles schaffen?

Wie so oft wurde zuletzt nicht alles so heiß gegessen wie es gekocht wurde. Aber, um in der Metapher zu bleiben, zeigte sich später, dass die Suppe doch recht schmackhaft war: Die Qualität verbesserte sich in den Unternehmen, nicht nur im Hinblick auf den Datenschutz, sondern auch bzgl. der Informationssicherheit und der allgemeinen Organisationsstrukturen im Unternehmen... zumindest bei den durch die UIMC betreuten Institutionen.

Nun stehen schweizerische Unternehmen vor der gleichen oder zumindest sehr ähnlichen Herausforderung, bis zum 1. September 2023 eine neue gesetzliche Grundlage im Datenschutz umzusetzen. Da sich das revisionierte Datenschutzgesetz (rDSG) stark an der DSGVO orientiert hat, ist mehr als naheliegend, von der Erfahrungen dieser Umsetzung zu profitieren.

Innerhalb dieses Whitepapers wollen wir Ihnen die Änderungen durch das revisionierte Datenschutzgesetz und die Möglichkeiten aufzeigen, wie Sie diese Anforderungen möglichst pragmatisch umsetzen können.

Dr. Heiko Haaz
Partner der UIMC und
Geschäftsfeldleiter Datenschutz

Allgemeines

Die Ausführungen betrachten die Änderungen, die durch das In-Kraft-Treten des neuen Schweizer DSG am 1. September 2023 aufkommen. Verglichen wird dies im Nachfolgenden mit der bisherigen Vorgehensweise der Orientierung an den Normen der DSGVO, die durch ihre exterritoriale Wirkung auch in der Schweiz Anwendung finden kann.

Dadurch wurde letztlich eruiert, inwiefern aktueller Handlungsbedarf durch mögliche Änderungen der neuen Rechtslage gegeben ist, wenn bisher eine Orientierung an der DSGVO erfolgte. Dargestellt werden die wesentlichen Veränderungen und deren Auswirkungen.

Anwendungsbereich des DSG

Der persönliche Anwendungsbereich wurde verkleinert und gilt nunmehr nur noch für personenbezogene Daten. Dadurch wurde der Schutz der Daten von juristischen Personen aus dem Gesetz entfernt. Insofern ergibt sich eine Reduzierung des Anwendungsbereichs in Bezug auf die geschützten Daten.

Hierdurch ergibt sich kein aktueller Handlungsbedarf, weil durch die Einschränkung keine Erweiterung der zu schützenden Daten eingetreten ist. Zu beachten gilt jedoch, dass bei der Verarbeitung von Unternehmensdaten im B2B-Bereich dennoch meist personenbezogene Daten der Ansprechpartner verarbeitet werden. Ebenso gilt es zu beachten, dass andere gesetzliche Vorgaben dennoch die Verwendung der nicht vom DSG erfassten Daten beschränken können, wie beispielsweise durch den Persönlichkeitsschutz nach Art. 28 ZGB, den Schutz des Geschäfts- und Fabrikationsgeheimnis nach Art. 162 StGB sowie Bestimmungen nach dem UWG.

Der räumliche Geltungsbereich wurde – ähnlich der DSGVO – ausgedehnt, jedoch erzeugt dies keinen Handlungsbedarf für Schweizer Gesellschaften. Dies betrifft insbesondere Gesellschaften außerhalb der Schweiz, deren Datenverarbeitung sich in der Schweiz auswirkt bzw. Personen in der Schweiz betrifft.

Begriffsbestimmungen

Dem Bereich der besonders schützenswerten personenbezogenen Daten wurden – anders als in der DSGVO – auch Daten über die Intimsphäre betroffener Personen und Daten über Maßnahmen der sozialen Hilfe hinzugefügt. Ebenso wurde diese um Daten über die Ethnie, genetische Daten sowie biometrische Daten, die eine natürliche Person eindeutig identifizieren erweitert.

Daten der Intimsphäre Betroffener dürfte bei der Datenverarbeitung häufig weniger eine Rolle spielen, doch sind ggfs. Daten über Maßnahmen der sozialen Hilfe zu berücksichtigen. Daten über die Ethnie, genetische sowie biometrische Daten wurden ggfs. bereits durch einen Umsetzungsmaßstab nach der DSGVO bei exterritorialer Wirkung dieser berücksichtigt, was unternehmensintern jedoch zu prüfen ist, um Verfehlungen in diesem Bereich zu vermeiden.

Eingeführt wurde eine Regelung zum Profiling, die sich an der Regelung der DSGVO orientiert. Zusätzlich gibt es im Schweizer DSG eine Regelung zum Profiling mit hohem Risiko, welches an eine Einwilligung der Betroffenen geknüpft wird. Dies liegt vor, wenn eine Verknüpfung von Daten vorgenommen wird, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit von natürlichen Personen zulässt. Hier ist zu prüfen, ob solche Handlungen gesetzt werden, um eruieren zu können, ob Einwilligungen einzuholen sind.

Der Begriff Auftragsverarbeiter aus der DSGVO wurde im DSG als Auftragsbearbeiter eingeführt. Handlungsbedarf entsteht hierbei jedoch nicht, weil die Bezeichnung keine Auswirkungen auf zu treffende Maßnahmen hat.

Zulässigkeit der Datenverarbeitung

Grundsätze des DSG

In diesem Artikel wurden Regelungen an die Voraussetzungen an eine rechtsgültige Einwilligung aufgenommen. Diese Regelungen entsprechen denen der DSGVO, weshalb dies bei einer internen Prüfung zu berücksichtigen ist und eine Umsetzung bereits sichergestellt sein kann.

Berücksichtigt werden muss dabei, dass die Einwilligung als solche klar erkennbar und von anderen Sachverhalten abgegrenzt ist und die Informationen über die Datenverarbeitung vollständig vorliegen (Stichwort: Informiertheit der Einwilligung).

Ausdrückliche Einwilligungen sind jedenfalls erforderlich für:

- die Bearbeitung von besonders schützenswerten Personendaten;
- ein Profiling mit hohem Risiko durch private Personen; oder
- ein Profiling durch Bundesorgane.

Rechtfertigungsgründe

Wie die Rechtsgrundlagen nach der DSGVO sind auch nach dem Schweizer DSG Rechtfertigungsgründe für Datenverarbeitungen und somit der Erlaubnis von Datenverarbeitungen ohne die Begehung einer Persönlichkeitsverletzung enthalten, die im Zusammenhang mit Datenverarbeitungen auf ihre Anwendbarkeit zu prüfen sind.

Anders als nach der DSGVO sind diese jedoch nicht zwingend in Informationspflichten bzw. bei Auskunftsersuchen zu nennen, doch kann es ratsam sein, dies in konkreten Fällen zu tun, weil insbesondere bei den Informationspflichten die Liste nicht abschließend ist.

Werden Datenverarbeitungen von Schweizer Gesellschaften auch ins Ausland angeboten/erbracht, ergibt sich hieraus noch kein zwingender Handlungsbedarf, weil dann die Informationspflichten nach der DSGVO erfüllt werden, die denen nach dem DSG in geeigneter Weise entsprechen. Bei rein innerstaatlichen Sachverhalten ist eine Ergänzung bzw. Änderung der Informationspflichten und dementsprechend eine Anpassung auf das Schweizer DSG möglich.

Bonitätsprüfung

Neu ist hier der Rechtfertigungsgrund zur Bonitätsprüfung, der – wenn solche vorgenommen werden sollen – zu prüfen ist, weil der Rechtfertigungsgrund bestimmte Voraussetzungen zur Zulässigkeit normiert (siehe Art. 31 Abs. 2 lit. c. DSG).

Erlaubt ist eine Kreditwürdigkeitsprüfung nur unter folgenden Voraussetzungen:

- Es handelt sich weder um besonders schützenswerte Personendaten noch um ein Profiling mit hohem Risiko.
- Die Daten werden Dritten nur bekanntgegeben, wenn diese die Daten für den Abschluss oder die Abwicklung eines Vertrags mit der betroffenen Person benötigen.
- Die Daten sind nicht älter als zehn Jahre.
- Die betroffene Person ist volljährig.

Automatisierte Einzelentscheidung

Relativ analog zu der Regelung der DSGVO wurde ein Passus eingefügt, der die Zulässigkeit von automatisierten Einzelentscheidungen begrenzt. Aufgrund der Komplexität solcher Sachverhalte wird auf eine eingehendere Darstellung verzichtet.

Wichtig ist zu erkennen, ob solche Entscheidungen getroffen werden und welche Pflichten damit einhergehen. Die Folge sind nämlich erweiterte Informationspflichten, weil über die Entscheidung selbst und deren Automatisierung informiert werden muss, um dem Betroffenen die Möglichkeit zur Stellungnahme zu geben und um zu verlangen, dass die Entscheidung von einer natürlichen Person geprüft wird. Auch bei diesem Tatbestand können Ausnahmen in Betracht gezogen werden, die in Einzelfallprüfungen zu beurteilen sind.

Sicherheit der Datenverarbeitung

Die Sicherheit hat nun einen höheren Stellenwert erhalten. Dies zeigt sich einerseits daran, dass die Pflicht, geeignete technische und organisatorische Maßnahmen umzusetzen, als Grundsatz aufgenommen wurde. Andererseits werden auch Prinzipien wie „Privacy by Design“ und „Privacy by Default“ eingeführt. Auch ist eine Pflicht zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen Maßnahmen eingeführt worden.

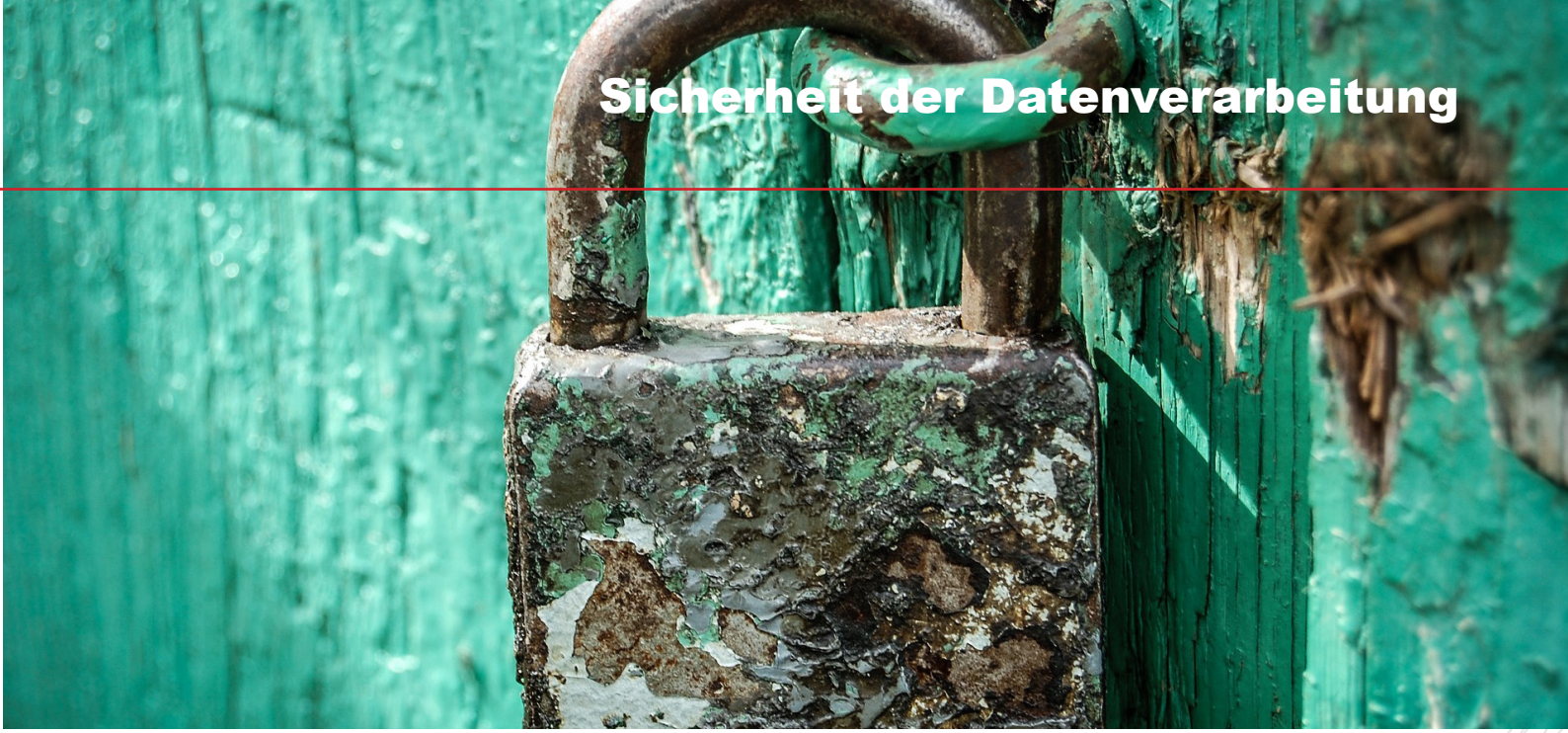
Bislang waren technischen und organisatorischen Maßnahmen nur erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Künftig sind bei der Abwägung neben der Art der Daten auch Zweck der Verarbeitung und der Stand der Technik zu berücksichtigen. Auch muss das ausgehende Risiko zur Beeinträchtigung von Persönlichkeits- und Freiheitsrechten berücksichtigt werden. Die Abschätzung des Risikos ist Vorbereitung und Ergebnis einer Datenschutz-Folgenabschätzung.

Neu ist die Forderung von speziellen Techniken wie die Pseudonymisierung und die Verschlüsselung von personenbezogenen Daten. Auch werden künftig Sicherheitsziele statt Kontrollmaßnahmen in den Fokus gestellt: Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste. Dies ist eine Terminologie, die aus der Informationssicherheit und den korrespondierenden Normen (z. B. ISO 27001) entnommen sind und demnach auch zeitgemäßer sind.

Ferner gilt, dass „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“ einzurichten ist. Somit sind regelmäßig Audits, Revisionen oder gar Penetrationstests durchzuführen. Dies ist auch schon heute die Herangehensweise der UIMC.

Privacy by Design/by Default

Neu ist Art. 7 DSG, der Verantwortliche zur Einhaltung bestimmter technischer und organisatorischer Maßnahmen zwingt, um die Datenverarbeitungsgrundsätze des neuen DSG einhalten zu können. Datenverarbeitungen müssten somit geprüft werden, ob damit die Vorgaben erfüllt werden können. Vor allem wird dies Unternehmen betreffen, die selbst Software entwickeln, weil diese Vorschriften dann bereits im Entwicklungsstadium einzuplanen sind.



Der EDÖB schreibt hierzu:

> *„Der Datenschutz durch Technik verlangt, dass sie ihre Applikationen u.a. so ausgestalten, dass die Daten standardmässig anonymisiert oder gelöscht werden. Datenschutzfreundliche Voreinstellungen schützen die Nutzer von privaten Online-Angeboten, die sich weder mit Nutzungsbedingungen noch den daraus abzuleitenden Widerspruchsrechten auseinandergesetzt haben, indem nur die für den Verwendungszweck unbedingt nötigen Daten bearbeitet werden, solange sie nicht aktiv werden und weitergehende Bearbeitungen autorisieren.“*

Bei der Einhaltung dieser Vorschriften kann ein Datenschutzberater hilfreich zur Seite stehen und eine beratende Stellung in der Produkterstellung einnehmen.

Datenschutz-Folgenabschätzung

Neu eingeführt wurde die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung, wenn die Voraussetzungen dafür vorliegen. Diese sind etwas eingeschränkter als nach der DSGVO, können jedoch entsprechend angewendet werden.

Dadurch kann sich ein möglicher Handlungsbedarf in Schweizer Gesellschaften ergeben, wenn diese nicht bereits nach dem Maßstab der DSGVO die Notwendigkeit von Datenschutz-Folgenabschätzungen eruiert haben. Dies kann vor allem dann der Fall sein, wenn eine mittelbare Anwendung der DSGVO bereits vorhanden war oder ein Konzernverbund besteht, dessen gemeinsame Datenverarbeitungen innerhalb der EU diesen Prüfkriterien unterzogen wurde. Eine Prüfung der internen Datenverarbeitungen auf diese gesetzliche Verpflichtung wird empfohlen.

Der EDÖB merkt an, dass allgemein gehaltene Datenschutz-Folgenabschätzungen, die Risiken nicht ordnungsgemäß behandeln, nicht ausreichend sind. Hierzu kann der EDÖB bei Einwänden gegen die erstellte Datenschutz-Folgenabschätzung Präzisierungen bzw. Ergänzungen nahelegen.

Datenschutz-Organisation

Datenschutzberater

Ähnlich der DSGVO gibt es die Möglichkeit, einen Datenschutzbeauftragten zu bestellen, der in der Schweizer Terminologie Datenschutzberater genannt wird. Damit einhergehend kann eine Ausnahme bei der Konsultation der Aufsichtsbehörde genutzt werden, wenn bestimmte Voraussetzungen zutreffen.

Nicht nur die genannte Erleichterung kann hierbei in Anspruch genommen werden, sondern auch umfassendes Know-How in der praktischen Umsetzung der datenschutzrechtlichen Bestimmungen. Hierbei ist auf die entsprechende Fachkunde des Datenschutzberaters zu achten, die zur Ernennung zum Datenschutzberater vorliegen muss, um die o. g. Ausnahme in Anspruch nehmen zu können.

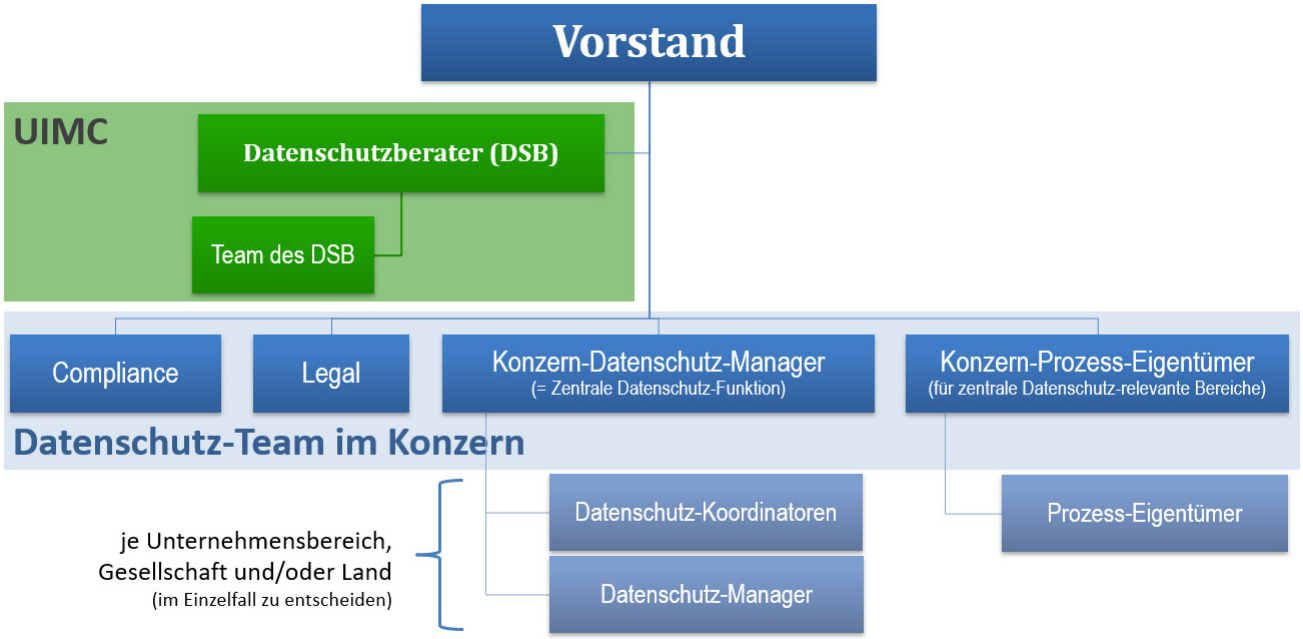


Abb.: Aufbau-Organisation (kann in KMU wesentlich schlanker gestaltet werden)

Konsultation des EDÖB

Wie in der DSGVO ebenso vorgesehen, muss im Fall einer Datenschutz-Folgenabschätzung dann, wenn diese zu keiner Herabsetzung des Risikos führte, der EDÖB konsultiert werden.

Hier ergibt sich jedoch eine Erleichterung, wenn ein Datenschutzberater benannt ist. Alternativ zum EDÖB kann dieser konsultiert werden, wodurch von der Einbindung des EDÖB abgesehen werden kann. Eine Einbindung ist zu dokumentieren.

Vorgehensweise der UIMC

Das prinzipielle Vorgehen der UIMC in der Beratung zeichnet sich durch eine Mischung aus vorstrukturierten und standardisierten Verfahrensweisen mit unterstützenden Hilfsmitteln sowie individuellen Problemlösungen aus. Hierbei hat sich ein top-down-orientiertes Vorge-hensmodell bewährt, das in Anlehnung an gängige Standards erarbeitet worden ist.

Nach erfolgter Analyse wird in Form eines Maßnahmenkatalogs ein Umsetzungskonzept erarbeitet und eine Datenschutz-Organisation bzw. ein Datenschutz-Managementsystem aufgebaut. In Form der Regelbetreuung werden neben einer Projektverfolgung Adhoc-Anfragen bearbeitet, regelmäßige Abstimmungen und Revisionen vorgenommen sowie eine Umsetzung vorangetrieben (inkl. Schulungen). Auch findet ein regelmäßiges Reporting inkl. eines jährlichen Tätigkeitsberichts an die Geschäftsführung statt.

Abb.: Vorgehensweise der UIMC

Verzeichnis von Bearbeitungstätigkeiten

Das Führen von Verzeichnissen von Bearbeitungstätigkeiten stellt eine neue Pflicht nach dem DSG dar. Hierdurch müssen Verzeichnisse mit bestimmten Pflichtinhalten geführt werden, die die Verfahren im eigenen Hause abbilden.

Weil die Anforderungen an den Inhalt nicht ganz so hoch sind, wie nach der DSGVO, können etwaige Anpassungserfordernisse entfallen, doch sollten bestehenden Verzeichnisse von Verarbeitungstätigkeiten auf mögliche Ergänzungserfordernisse geprüft werden.

Je nach Betätigungsfeld des Unternehmens muss in Betracht gezogen werden, die Erfordernisse der DSGVO erfüllen zu müssen, wodurch sich ein Ergänzungsbedarf ergeben kann. Ratsam kann überdies die Führung eines Verzeichnisses von Verarbeitungstätigkeiten nach den Vorgaben der DSGVO sein, weil dieses einen wesentlichen Beitrag zur Einhaltung der restlichen Bestimmungen als „Fundament“ leisten kann.

Datentransfer

Datentransfer ins Ausland

Die Norm wurde leicht verändert, doch besteht im Wesentlichen derselbe Inhalt und dieser entspricht den Regelungen der DSGVO. Dabei besteht weiterhin die Möglichkeit, Standardvertragsklauseln der EU für solche Datentransfers zu verwenden.

Der EDÖB schreibt hierzu:

> *„Bereits unter der DSGVO genehmigte Standardklauseln der Europäischen Kommission werden vom EDÖB anerkannt.“*

Bei der Verwendung der neuen Standardvertragsklauseln ist darauf zu achten, dass der entsprechend richtige Anwendungsfall hinsichtlich der Module in den Standardvertragsklauseln gewählt wird. Ebenso ist zu eruieren, inwiefern auf den entsprechenden Vertrag sowohl die DSGVO als auch das DSG anwendbar sind, weil ggfs. Anpassungen notwendig sein können.

Die Weiterführung der bisherigen Anerkennungspraxis der Standardvertragsklauseln kann also weiterhin angenommen werden. Dies bringt vor allem bei Gruppen- und Konzernverträgen erhebliche Erleichterungen mit sich, wenn sich innerhalb der Gruppe bzw. des Konzerns Schweizer Gesellschaften befinden, wodurch für diese kein separater Vertrag abzuschließen ist.

Rechte der Betroffenen

Informationspflichten

Die Informationspflichten wurden im Vergleich zu den Vorgängerregelungen ausgebaut, enthalten jedoch keine abschließende Liste an zu erteilenden Informationen und ebenso wenig eine Regelung zur konkreten Erteilung der Informationen. Hierdurch entsteht Formfreiheit der Mitteilung an Betroffene. Etwas erweitert gegenüber der DSGVO sind die Ausnahmen von der Informationspflicht, die teilweise entfallen oder aber eingeschränkt, aufgeschoben oder darauf verzichtet werden kann, wenn bestimmte Voraussetzungen vorliegen. Weil die Voraussetzungen regelmäßig nicht greifen dürften, sollte die Informationserteilung stets erfolgen, um hier gesetzeskonform zu agieren. Einzelfallprüfungen können vorgenommen werden, um die Ausnahmen nach Art. 20 DSG zu eruieren.

Die Informationspflichten übersteigen die Pflichten nach der DSGVO kaum. Weitergehende Informationen sind nur im Bereich der Drittlandtransfers zu erkennen, bei denen der konkrete Empfängerstaat bezeichnet werden muss, während die restlichen Informationspflichten hinter den Vorgaben der DSGVO zurückbleiben. Insofern ergibt sich hier minimaler Handlungsbedarf, sofern bereits nach den DSGVO-Bestimmungen informiert wird.

Betroffenenrechte

Im Zuge der Neugestaltung des DSG wurden die Betroffenenrechte weiter gestärkt und ausgebaut.

Dabei wurde das Auskunftsrecht im Gegensatz zu den alten Regelungen erweitert und an die DSGVO angeglichen.. Das Recht auf Datenübertragbarkeit wurde neu eingefügt, was letztlich jedoch ebenso der DSGVO entspricht. Für beide Betroffenenrechte gibt es Einschränkungstatbestände, die im Einzelfall geprüft werden könnten und die etwas weiter sind als die Bestimmungen nach der DSGVO (z. B. auch umfasst sind „offensichtlich querulatorische“ Auskunftsersuchen). Weitere Ansprüche auf Löschung, Berichtigung, Verbot der Verarbeitung und die Versagung der Bekanntgabe an Dritte wurden indirekt ebenso aufgenommen (Art. 32 DSG)

Klar definiert wurde über die Verordnung zum Datenschutz (DSV) in Art. 18 die Frist zur Bearbeitung von entsprechenden Anfragen zu Auskunft und zur Datenübertragung von Betroffenen, die mit 30 Tagen angegeben wird. Es liegt nahe, diese Frist auch für die indirekt enthaltenen Betroffenenrechte in Betracht zu ziehen.

Ein Vorgehen nach den Bestimmungen der DSGVO kann hier beibehalten werden, sofern ein solches besteht. Ansonsten sind Maßnahmen zu treffen, um im Anlassfall die Betroffenenrechte erfüllen zu können. Gegebenenfalls können im Einzelfall Ausnahmebestimmungen geprüft werden, die teilweise etwas weiter sind.

Datenpannen

Meldung von Verletzungen der Datensicherheit

Die Meldepflicht von Datenschutzverstößen ist in der Meldeschwelle etwas anders gelagert als nach der DSGVO und wurde neu eingeführt. Dies ist bei der Prüfung etwaiger Vorfälle zu berücksichtigen. Nämlich wird eine Meldepflicht erst dann ausgelöst, wenn die Verletzung der Datensicherheit voraussichtlich zu einem hohen Risiko für die Betroffenen führt. Nach der DSGVO wäre in einem solchen Falle die Benachrichtigung der Betroffenen zusätzlich zur aufsichtsbehördlichen Meldung vorgesehen. Die Betroffenen sind nach dem DSG jedoch dann zu informieren, wenn es zu ihrem Schutze erforderlich ist oder der EDÖB dies verlangt.

Der EDÖB gibt zusätzlich die Information an die Hand, dass nur eingetretene Persönlichkeits- oder Grundrechtsverletzungen meldepflichtig sind, nicht jedoch erfolgreich abgewehrte oder untaugliche Cyberangriffe. Der Verantwortliche hat hierzu eine Prognose zu erstellen und eine Beurteilung vorzunehmen.

Ebenso ist die Frist nicht analog zur DSGVO angelegt, sondern als eine Meldung „so rasch wie möglich“ ohne die Bestimmung einer konkreten Frist. Es bleibt abzuwarten, wie der Begriff letztlich ausgelegt werden wird, eine Orientierung an der 72-Stunden-Maximalfrist der DSGVO erscheint sinnvoll zu sein.

Dies führt nicht unmittelbar zu einem Handlungsbedarf, sondern ist bei etwaigen Prüfungen von Datenschutzverletzungen zu beachten, um die weiteren Pflichten nach dem DSG zu bestimmen. Bei grenzüberschreitenden Vorgängen können sowohl die DSGVO als auch das DSG zu beachten sein, wenn gleichzeitig die betroffenen Daten bzw. Datenverarbeitungen beiden Rechtssystemen unterliegt. Hierbei handelt es sich jedoch um konkrete Einzelfallprüfungen.

Bei der Beurteilung von Datenschutzvorfällen, insbesondere bei der Risikoeinschätzung, sollte der Datenschutzberater eingebunden werden.


GF
DSB
IT
Fachbereiche
HR EK Mark. Fac.Mang. Prod.
Datenpanne/Verdacht, mitgeteilt durch externe Stelle oder interne Stelle an MA intern (siehe Anlage 1* und 2*)
Frist-Beginn
Vorprüfung durch den Datenschutz-Ansprechpartner im Hause
Info an DSB, Dokumentation (siehe Anlage 2*)
Vorfall IT bezogen?
Ja
Info an IT, Dokumentation (siehe Anlage 2*)
Gegenmaßnahmen prüfen und ergreifen
Nein
Dokumentation (siehe Anlage 2*)
Beratung: Wer ist Data Owner? Wer ist fachl. Verantwortlich?
Zusammenstellung der bekannten Infos
Notfallteam „Datenschutz“ (Beteiligung Marketing/PR opt.) (siehe Anlage 3*)
Bewertung des Sachverhalts
Beratung
Weitere Bewertung
weiter

Kontrollen und Strafen

Mitwirkungspflicht und Befugnisse des EDÖB

Verantwortliche haben dem EDÖB im Zuge seiner Ermittlungen alle Auskünfte zu erteilen sowie Unterlagen zur Verfügung zu stellen, die für die Ermittlung notwendig sind, widrigenfalls dieser folgendes anordnen kann:

- Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten, die für die Untersuchung erforderlich sind;
- Zugang zu Räumlichkeiten und Anlagen;
- Zeugeneivernahmen;
- Begutachtung durch Sachverständige.

Zum Vollzug der Maßnahmen kann der EDÖB auch kantonale oder kommunale Polizeiorgane beiziehen.

Auch in der DSGVO finden sich solche Mitwirkungspflichten von Verantwortlichen, die jedoch erst Handlungsbedarf nach sich ziehen, sofern dies im Zuge von Ermittlungen notwendig wird.

Hinzugekommen sind jedoch Befugnisse des EDÖB, die sich ebenso an der DSGVO orientieren. Anordnen kann der EDÖB, dass Bearbeitungen ganz oder teilweise angepasst, unterbrochen oder abgebrochen werden und dass Personendaten ganz oder teilweise gelöscht oder vernichtet werden. Zudem können Datenübertragungen ins Ausland aufgeschoben oder untersagt werden. Weitere Befugnisse zur Sicherstellung der Einhaltung des DSG sind vorbehalten (siehe Art. 51 DSG).

Wichtig zu wissen ist, wenn während einer Untersuchung des EDÖB erforderliche Maßnahmen zur Wiederherstellung der Einhaltung der Datenschutzvorschriften getroffen werden, so kann auch nur eine Verwarnung ausgesprochen werden.

Strafbestimmungen

Die Strafbestimmungen sehen Geldbußen bis zu 250.000,00 Schweizer Franken vor, die – anders als nach der DSGVO – nicht der verantwortlichen Stelle (dem Unternehmen) sondern vordergründig Leitungspersonen auferlegt werden können. Es ist aber nicht ausgeschlossen, dass Strafen Mitarbeitern ohne Leitungsfunktion auferlegt werden können. Zur Erfüllung der Tatbestände ist jedoch vorsätzliches Handeln eine Voraussetzung (siehe Art. 60 ff DSG).

Ausnahmen bilden Bußgelder bis zu 50.000,00 Schweizer Franken, wenn zur Ermittlung der strafbaren Personen Untersuchungsmaßnahmen bedingt sind, die auf die verwirkte Strafe unverhältnismäßig wären. Dann kann direkt der Geschäftsbetrieb verurteilt werden.

Bester Schutz vor Strafen:

Schulung und Sensibilisierung

Die Erfahrung zeigt, dass Vorgaben nur eingehalten werden, wenn Mitarbeiter die Hintergründe verstehen. Andernfalls werden entweder bewusst Regeln umgangen, weil sie als „lästig“ empfunden werden, oder es wird unbewusst aus Unwissen gegen diese verstoßen. So zeigt sich, dass viele Vorfälle durch nicht sensibilisierte oder unzureichend unterrichtete Mitarbeiter entstehen: Durch den sog. „unfreiwilligen Innentäter“.

Zur effektiven Umsetzung von Anforderungen ist es unerlässlich, die Mitarbeiter zu sensibilisieren und auf die zu ergreifenden Maßnahmen zu schulen. Unser eCollege ist eine webbasierte Schulungsplattform, die über das Internet ohne Aufbau eigener Infrastruktur erreichbar ist. Hiermit können Mitarbeiter im Datenschutz und in der Informationssicherheit sensibilisiert und geschult werden. Unabhängig, ob Sie im Büro, im Home-Office oder unterwegs sind.

Unsere Mission

Wir bringen unsere Fach-, Branchen- und Methodenkompetenz gewinnbringend ein, so dass praxisnahe Lösungen gefunden werden, die nicht nur den externen, sondern auch den internen Anforderungen des Geschäfts gerecht werden. Unsere Empfehlungen, bei deren Umsetzung wir tatkräftig unterstützen können, werden allen Beteiligten verständlich vermittelt, so dass Entscheidungen unter Berücksichtigung von Risiken und Zielen getroffen werden können. Dienstleistung bedeutet für uns auch, die Bedürfnisse unserer Kunden zu verstehen, um sie kompetent, schnell und auf Augenhöhe zu unterstützen.

Wir helfen Ihnen gerne...

pragmatisch; schließlich ist weder Datenschutz noch Informationssicherheit ein Selbstzweck. Vielmehr muss Ihr „Business“ weiter gut funktionieren. Dabei arbeiten wir lösungs- und dienstleistungsorientiert, indem wir flexibel auf Ihre Anforderungen und Bedürfnisse mit Best Practice eingehen. So entlasten wir Sie und Sie haben mehr Zeit für Ihr Tagesgeschäft.

erfahren, denn wir betreuen seit über 25 Jahren zufriedene Kunden. Unsere Berater/-innen können vielfältige Spezialisierungen nachweisen. Wir gehen strukturiert vor und weisen fachliche, methodische und Branchen-Expertise auf und setzen Tools effizienzsteigernd ein. So können Sie sich nachhaltig verbessern, weil unsere Lösungen praxiserprobt sind und regelmäßig überprüft werden. Dies stellen wir transparent dar, so dass Sie stets den Überblick behalten.

verständlich, indem wir komplizierte Dinge einfach erklären. Damit können wir verschiedene Interessensgruppen zusammenführen. Wir versuchen Menschen sympathisch zu überzeugen ohne zu überreden, weil wir Ihre Probleme verstehen wollen. Trockene Themen bringen wir lebendig rüber und realisieren dabei gemeinsam Ihre Ziele.

Datenschutz
Externe Datenschutzberater, Managementsystem, Auditierung, Folgenabschätzung, E-Learning

Informationssicherheit
Aufbau eines ISMS (ISO 27002, IT-Grundschutz, TISAX) bis zur Zertifizierungsreife

Organisation & Strategie
Prozess-Optimierung, Strategien, Konzepte

Wir stellen uns vor

Wir sind eine mittelständische Unternehmensberatung mit den Kerngebieten Datenschutz und Informationssicherheit. Im Jahr 1997 gegründet, gehören wir im Datenschutz zu den Marktführern und bieten als Vollsortimenter von einzelnen Tools bis hin zum Komplett-Outsourcing in Form einer externen Datenschutzberatung sämtliche Unterstützungsmöglichkeiten der Analyse, Beratung, Umsetzung und Schulung an.

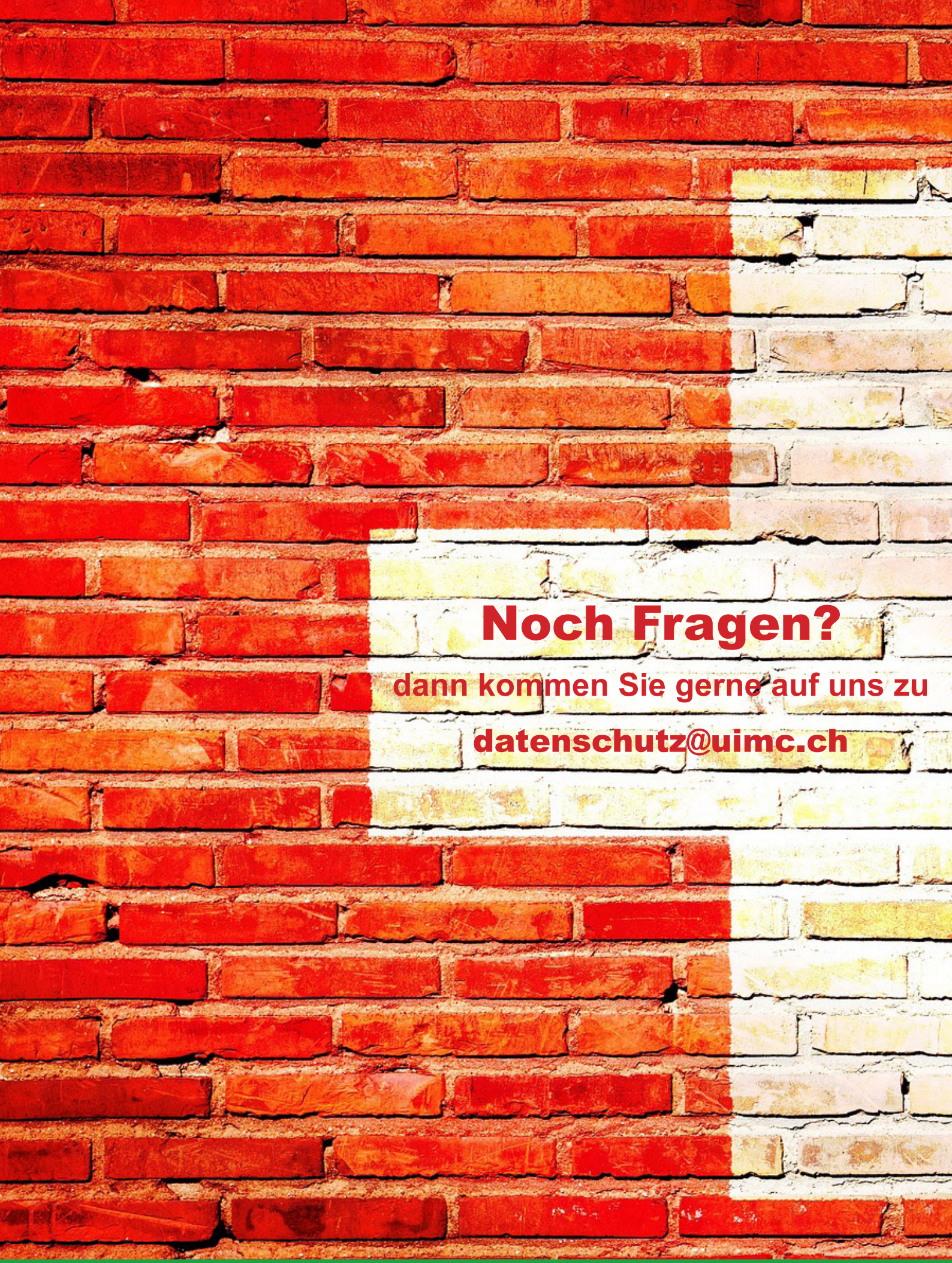
Unsere rund 30 Mitarbeiterinnen und Mitarbeitern haben breit gefächerte Spezialisierungen, die für praxisnahe Lösungen führen. Dies erlaubt es uns, größere Projekt ohne Abhängigkeit von einzelnen Mitarbeitern durchzuführen, aber auch ohne dabei die Flexibilität als Mittelständler zu verlieren, um auf Ihre individuellen Bedürfnisse eingehen zu können. Diese Expertise können wir nachweisen. Auch die Nähe zu unserer „Zertifizierungsschwester“ bringen wir zum Nutzen unserer Kunden ein.

Die auch aufgrund der hohen Qualität und Zufriedenheit langfristigen Kundenbeziehungen haben zu einer stetigen Ausdehnung unseres regionalen und fachlichen Tätigkeitsgebiets geführt. Hierbei legen die Inhaber nicht nur Wert auf solides, sondern auch auf nachhaltiges Wachstum (sowohl bei den Kunden als auch bei der Belegschaft). Für uns selbstverständlich, ist sich die UIMC auch Ihrer sozialen Verantwortung sehr bewusst. Auch genießt die Ausbildung bei uns einen großen Stellenwert.

Besser UIMC fragen.

pragmatisch.erfahren.verständlich.

Ihr Ansprechpartner für das rDSG
Tim Hoffmann


Noch Fragen?
dann kommen Sie gerne auf uns zu
datenschutz@uimc.ch