„Datenschutz in die DNA des Unternehmens einfügen“

Roundtable mit Dr. Christian Hamann, Gleiss Lutz, Barbara Schmitz, Osram, und Nikola Zacherl, MTU Aero Engines

Seit dem 25. Mai sorgt ein neues EU-Recht für Umbruch am Markt: die Datenschutz-Grundverordnung (DSGVO). Sie soll EU-weit die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen vereinheitlichen. Ziel ist der Schutz persönlicher Daten und die Gewährleistung des Datenverkehrs innerhalb Europas. Welche Auswirkungen hat die Verordnung auf Namensaktien? Das und vieles mehr beantworten Datenschutzexperten beim Roundtable des GoingPublic Magazins.

GoingPublic: Liebe Gesprächskreisteilnehmer, was ändert sich mit der Datenschutz-Grundverordnung (DSGVO), die seit dem 25. Mai in Kraft ist, insbesondere für Emittenten?

Dr. Hamann: Was sich u.a. verändern wird, ist der Umgang mit der Dokumentation der Verarbeitung von personenbezogenen Daten. Sehr spürbar werden auch die Veränderungen beim Behördenvollzug und im Bereich Sanktionen. Wir hatten bislang schon sehr strenge Datenschutzregeln, aber ab jetzt können richtig hohe Geldbußen folgen. Im schlimmsten Fall 4% des Jahresumsatzes. Natürlich sorgt das aktuell für viel Aufruhr am Markt.

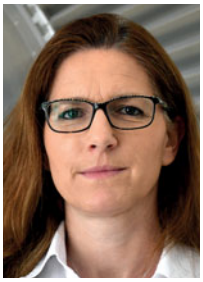
Schmitz: Dem stimme ich zu. Vor der Festlegung der DSGVO war Datenschutz zwar natürlich auch ein großes Thema bei den Aktiengesellschaften, doch es wurde kein „Zwang“ in diesem Zusammenhang auferlegt. Durch die DSGVO hat man jetzt keine Wahl mehr. In der Praxis ist die Dokumentationspflicht die gravierendste Änderung. Hier wird es künftig erheblich mehr Aufwand geben. Aus Datenschutzgesichtspunkten finde ich das neue Gesetz übrigens komplett richtig, denn in anderen Geschäftsbereichen haben wir solche Dokumentationspflichten ja auch schon längst.

Zacherl: Die DSGVO wird sich deutlich auf die Prozesse innerhalb der Unternehmen auswirken. Vieles wird künftig formalisierter ablaufen und intensiver dokumentiert werden. Insgesamt wird dadurch der interne Aufwand natürlich größer.

Unklarheiten gibt es vor allem noch bei Namens- und Inhaberaktien, da hier oft mehrere Akteure beteiligt sind, wie u.a. Banken und Emittenten. Hier stellen sich die Fragen: Wer ist überhaupt in der Pflicht, die Daten zu erheben, und wer muss die Aktionäre informieren? Bank oder Emittent?

Dr. Hamann: Einer der Schwerpunkte der DSGVO ist die Transparenzpflicht, die viel ausführlicher geregelt ist als bisher. Art. 13 DSGVO verpflichtet jeden, der Daten direkt von einer betreffenden Person – hier also einem Aktionär – erhebt,

> *Die DSGVO wird sich deutlich auf die Prozesse innerhalb der Unternehmen auswirken.*
>
> **Nikola Zacherl**



ZU DEN INTERVIEWPARTNERN

Dr. Christian Hamann ist Rechtsanwalt bei **Gleiss Lutz** in Berlin. Er berät nationale und internationale Mandanten zu allen Fragen des Umgangs mit personenbezogenen Informationen.

Barbara Schmitz leitet den Konzerndatenschutz bei **OSRAM** in München und ist seit Langem als Unternehmensjuristin im betrieblichen Datenschutz tätig. Sie ist zudem Autorin zahlreicher Buch- und Zeitschriftenbeiträge zum Datenschutz und regelmäßig Referentin von Seminaren und Fachtagungen.

Nikola Zacherl, Syndikusrechtsanwältin, ist seit 2006 Leiterin Recht beim Triebwerkshersteller **MTU Aero Engines** in München.

V.l.n.r.: Christof Schwab, Svenja Liebig, Nikola Zacherl, Dr. Christian Hamann und Barbara Schmitz.

den Betreffenden detailliert über die Verwendung der Daten und seine Rechte zu informieren. Nun bekommen Aktiengesellschaften in der Regel personenbezogene Daten nicht direkt von den Aktionären, sondern von den depotführenden Banken. Für solche Fälle einer Datenerhebung aus „anderen Quellen" schreibt Art. 14 DSGVO auch eine Informationspflicht vor. Diese gilt allerdings nicht für Informationen, die dem Betreffenden bereits vorliegen. Damit stellt sich für Aktiengesellschaften die Frage, ob und inwieweit sie sich darauf verlassen können, dass die Banken, die ja ihrerseits auch nach Art. 13 DSGVO informationspflichtig sind, den Aktionären bereits alles Notwendige mitgeteilt haben.

Nochmal zusammengefasst und aus rein praktischer Sicht: Wenn ich eine Namensaktie bei einer Gesellschaft kaufe – von wem und in welcher Form werde ich über die Datenerhebung informiert werden?

Schmitz: Wenn wir als Emittent von der Bank die Information bekommen haben, dass jemand Namensaktien gekauft hat, kann ich davon ausgehen, dass derjenige auch ausführliche Informationen über das Unternehmen bekommt. Das schließt auch die Datenschutzinformationen mit ein. In dem Fall würde Art. 14 Abs. 5 greifen, der Ausnahmefälle festlegt. Dieser Artikel besagt, dass nicht jeder individuell über die Neuerung im Datenschutz informiert werden muss, sondern es reicht aus, über die Website, z.B. im IR-Bereich, explizit zu informieren. Dies handhaben wir auch in der Praxis so. Zudem wird in unserer allgemeinen Daten-Policy nochmals über die neuen Richtlinien informiert. Kritisch sehe ich jedoch in der Tat, dass nicht unbedingt jeder Aktionär einen Internetzugang hat, vor allem ältere Generationen. Da habe ich ehrlich gesagt noch keine allgemeingültige Lösung gefunden.

Wird denn bei den Banken überhaupt daran gearbeitet, umfassender zu informieren?

Dr. Hamann: Ja. Die Banken haben alle ihre Datenschutz-Policies, Hinweise und Erklärungen ganz genau angeschaut. Insofern sind schon Bemühungen seitens der Banken da. Allerdings werden die Banken nicht alles abdecken können, wofür die Aktiengesellschaften informationspflichtig sind, z.B. Angaben zu eingebundenen Dienstleistern oder die Kontaktdaten des Datenschutzbeauftragten der Gesellschaft.

Zacherl: Grundsätzlich ist es so, dass ein Emittent keine Übersicht hat, über welche Bank der Aktionär seine Namensaktie kauft. Um sich auf die Information des Aktionärs durch die Depotbank verlassen zu können, müsste man das bei jeder Bank abfragen. Das ist aufgrund der vielen Depotbanken praktisch unmöglich. Viele Käufe werden zudem übers Ausland getätigt – das macht es noch schwieriger.

Hamann: Laut Art. 14 Abs. 5c) DSGVO greift außerdem eine Ausnahme von der Informationspflicht, wenn die Gesellschaft die Daten auf der Grundlage einer ausdrücklichen gesetzlichen Regelung erhält. Das ist z.B. der Fall bei den Daten, die die Depotbanken den Aktiengesellschaften gem. § 67 Abs. 4 AktG für die Zwecke des Aktienregisters übermitteln müssen.

Wie bereits erwähnt ist im Artikel 67.1 AktG die Übermittlung der Daten von Namensaktien gesetzlich verankert. Eine Ausnahme bildet die Nationalität, die dort nicht explizit aufgeführt wird. Würde dieser Bereich dazu führen, dass man durch die DSGVO den Neuaktionär künftig darüber informieren muss, dass man seine Nationalität erhebt?

Dr. Hamann: Zunächst braucht man da als Gesellschaft einen legitimen Zweck und eine gesetzliche Grundlage, um diese Daten erheben zu dürfen. Das können bei einem Datum wie Nationalität Compliance-Pflichten sein oder Maßnahmen gegen Geldwäsche. Allerdings ist bei der Geldwäsche eher der Wohnsitz als die Nationalität entscheidend. Im Hinblick auf Terrorlisten u.Ä. sollte man ggf. etwas genauer auf die Nationalität schauen, ohne natürlich bestimmte Ethnien zu diskriminieren. Aber das ist eine ziemliche Grauzone. Wenn ich als Gesellschaft berechtigt bin, Informationen zur Nationalität o.Ä. zu erheben, muss ich über die beabsichtigte Verwendung auch gem. Art. 13 oder 14 DSGVO informieren.

Schmitz: Hierzu möchte ich noch ergänzen, dass der Aspekt der Nationalität mit

Noch sorgt die DSGVO für Wirbel am Markt - in ein paar Jahren wird allerdings auch hier Normalität einkehren, sind sich die Experten sicher.

der DSGVO nicht neu hinzugekommen ist. Für einige Aspekte wie Terrorlisten oder Compliance muss die Nationalität natürlich überprüft werden. Aber dazu kann man ja auch ein milderes Mittel anwenden. Von daher müsste man nochmal den Aspekt der Nationalität überdenken. Jedoch kommt hier der risikobasierte Ansatz der DSGVO schon zum Vorschein. In dem oben genannten Fall sieht man deutlich, dass das Risiko der Privatsphärenmissachtung nicht hoch ist. Von daher finde ich die beiden Kombinationen aus Personenbezug und risikobasiertem Ansatz sehr hilfreich.

Gesetzt den Fall, es gibt ein Merkmal, das nicht durch Art. 67.1 gedeckt ist: Beurteilen Sie die Informationspflicht durch die DSGVO überhaupt als verhältnismäßig?

Zacherl: Die eigentliche Frage ist doch diese: Welche Art der Information ist verhältnismäßig? Und wie erfülle ich dies auf eine praktikable Art und Weise? Zunächst ist anzumerken, dass eine Information bei der Datenerhebung selbst ausscheidet. Der Emittent muss daher im Nachgang informieren. Hier stellt sich jetzt die Frage: durch welches Medium?

Schmitz: Ohne Nationalität würde man es über Ausnahmeregeln klären – hier würde dann ein Verweis zum Link auf die Website mit der DSGVO und der Privacy Policy reichen, in der explizit aufgeführt wird, warum man gewisse Daten wie Nationalität erhebt. Falls in dem Fall eine Aufsichtsbehörde dies als unzureichend erklären würde, würde ich in dem Fall nochmal explizit aufführen, warum solche Datenerhebungen nicht die Privatsphäre des Einzelnen verletzen. Hier hätte man zumindest eine einheitliche Argumentationslinie und könnte dann für den Fall der Fälle doch die Informationspflicht anwenden, falls die Aufsichtsbehörde dagegen stimmt.

Dr. Hamann: Das sehe ich genauso. Kann ich Art. 14 Abs. 5c) DSGVO nicht anwenden, bin ich in der Pflicht zu informieren. Doch was heißt informieren? Muss ich jeden Einzelnen anschreiben oder reicht es aus, über die Website aufzuklären? Hier lässt die DSGVO die genaue Vorgehensweise offen. Bei den Aktionärsinformationen, über die wir hier sprechen, genügt m.E. ein prominent platzierter Hinweis auf der Website der Gesellschaft. Dies wäre dann ein verhältnismäßiger Aufwand – unverhältnismäßig wäre es z.B., wenn jeder einzelne Neuaktionär postalisch innerhalb eines Monats nach Erwerb seiner Aktien angeschrieben werden müsste.

Zacherl: Das ist ein entscheidender Punkt. Oft haben die Emittenten – wie etwa die MTU Aero Engines – keine E-Mail-Adressen erfasst, sodass auf jeden Fall ein postalischer Versand notwendig wäre. Für ein Aktionärsmailing besteht häufig keine interne Infrastruktur; hier müsste dann ein Dienstleister beauftragt werden, um die Kommunikation abzuwickeln. Das ist nicht nur aufwändig, sondern schafft datenschutzrechtlich eine neue Schnittstelle.

Ein wichtiger Punkt der DSGVO ist die Löschung der personenbezogenen Daten. Bezogen auf Namensaktien: Wann komme ich aus dem Aktienregister raus?

Schmitz: Aus meiner Sicht muss der Aktionär dann aus dem Aktienregister gelöscht werden, sobald dieser keiner mehr ist. Aus buchhalterischen und steuerlichen Gründen kann es aber durchaus sein, dass die Daten noch zum Nachweis aufbewahrt werden können. Da müssen dann entsprechend die Speicherungen nach dem Berechtigungs- und Rollenkonzept geändert werden. Aus den HGB-Grundlagen gilt ja eine generelle Löschfrist von zehn Jahren. Bei den hauptversammlungsbezogenen Daten gelten Löschfristen von drei Jahren, die sich allerdings im Falle von Rechtsstreitigkeiten verlängern würden.

Zu den Sanktionen: Sind 4% des Umsatzes ein „Schreckgespenst" für die Unternehmen?

Dr. Hamann: Wenn man alles richtig macht, hat man auch unter dem neuen Recht natürlich nichts zu befürchten. Das Problem ist nur – und das bestätigen sogar die Aufsichtsbehörden –, dass eine hundertprozentige Datenschutz-Compliance de facto nicht möglich ist. Es wird immer Grauzonen geben. Bislang sind die Erfahrungswerte so, dass die Aufsichtsbehörden

Bringt Licht ins Dunkel: Dr. Hamann klärt über Unklarheiten bei der neuen DSGVO auf.

Besonders bei Detailfragen sorgt das neue EU-Recht noch für einige Unklarheiten.

bei „Ersttätern“ erst mal eine Verwarnung ausgesprochen und die Möglichkeit zur Nachbesserung gegeben haben, bevor mit Bußgeldern operiert wurde. Wie sich das allerdings in Zukunft entwickeln wird, ist nicht ganz klar. Mit der neuen DSGVO haben die Behörden nämlich kein Opportunitätsermessen mehr, darüber zu entscheiden, ob sie überhaupt ein Bußgeld verhängen wollen. Es ist also gesetzlich festgelegt, dass auf jeden Fall ein Bußgeld verhängt wird – abgesehen von geringfügigen Verstößen. Es wird deshalb ganz sicher mehr Bußgelder geben und diese werden sich auch spürbar erhöhen.

In den oben geschilderten Fällen würde die Datenerhebung nicht aus kommerziellen Zwecken, sondern aus rein gesetzlichen Pflichten erfolgen. Wäre bei einem minimalen Verstoß oder einem Agieren in der Grauzone denn überhaupt mit Sanktionen zu rechnen?

Dr. Hamann: Wenn der „Verstoß“ allein darin besteht, dass Sie ordentlich zur HV einladen, aber den Link zu Ihren ebenfalls ordentlichen Datenschutzhinweisen auf der Website vergessen, dann bezweifele ich, dass hier tatsächlich Bußgelder drohen. Und falls doch, dann wird die Strafzahlung relativ gering sein. Falls allerdings die Daten Ihrer Aktionäre über Wochen hinweg im Internet frei zugänglich sind, weil Sie die Datensicherheit vernachlässigt haben, sieht das Ganze schon anders aus. Hier könnte es zuweilen richtig „wehtun“.

Schmitz: Der BGH hat erst letztes Jahr beschlossen, dass ein funktionierendes Compliance-Managementsystem sich bußgeldmindernd auswirken kann. Dies würde ich auch auf die DSGVO adaptieren. Wenn ich als Unternehmen eine funktionierende Dokumentation und Transparenzpflicht nachweisen kann, werden die Aufsichtsbehörden sicherlich Milde walten lassen. Das wird sich dann in diese Richtung einpendeln, wie wir es bereits vom Kartellrecht kennen.

> *Der BGH hat erst letztes Jahr beschlossen, dass ein funktionierendes Compliance-Managementsystem sich bußgeldmindernd auswirken kann.*
>
> **Barbara Schmitz**

Kurz und knapp zusammengefasst: Was bedeutet die DSVGO wirklich für einen Mehraufwand aus Sicht der Emittenten?

> *Interessant finde ich, dass die DSGVO ursprünglich mit dem Versprechen einer Entbürokratisierung angepriesen wurde.*
>
> **Dr. Christian Hamann**

Und wird die Diskussion in ein paar Jahren überhaupt noch Relevanz haben?

Dr. Hamann: Interessant finde ich, dass die DSGVO ursprünglich mit dem Versprechen einer Entbürokratisierung angepriesen wurde. Eingetreten ist das komplette Gegenteil: Der bürokratische Aufwand ist deutlich erhöht. Allerdings wird der Aufwand in dem Bereich, über den wir gesprochen haben – Informationen der Aktiengesellschaften an die Aktionäre im Bereich Namens- und Inhaberaktien – sicherlich überschaubar bleiben. Man muss nicht anfangen, jeden einzelnen Namensaktionär per Post über jede Verarbeitung seiner Daten zu informieren.

Schmitz: Das sehe ich ähnlich. Der entscheidende Punkt wird sein, dass man das Thema Datenschutz in die DNA des Unternehmens einfügt. Man sollte nicht anfangen, den Datenschutz neu zu erfinden, sondern diesen vielmehr im Unternehmen fest verankern – insofern sollte das eigentlich nichts Neues sein für die einzelnen Gesellschaften.

Zacherl: Ich bemerke eine gewisse Unruhe, weil es in vielen Detailfragen noch Unklarheiten gibt. Ich denke, dass das Ganze sich sicherlich in den nächsten Jahren einspielen und zum Alltag werden wird.

Liebe Teilnehmer, vielen Dank für die spannende Diskussionsrunde. ■

Das Gespräch führten Christof Schwab und Svenja Liebig.

Eine längere Version finden Sie auf **www.goingpublic.de**