1/2018
1 – 24

VfGH
Hohe Strafen von DSB?
Thomas Schweiger

# DATENSCHUTZ KONKRET

**Recht | Projekte | Lösungen**

Chefredaktion: Rainer Knyrim

# Kinder/Schüler und Datenschutz

## Bei WhatsApp sind den Schulen die Hände gebunden
*IInterview mit Johannes Thaler, Stadtschulrat Wien*

## Datenschutz – das ist wie ein Tropfen im See
*Interview mit Moritz Oman, Gymnasiast*

## Altersnachweis bei Kindern
*Verena Wlk*

## Digitalisierung: vernetztes Spielzeug und Internetspiele
*Karin Tien und Jennifer Maria Held*

## Judikatur: Nutzung von WhatsApp durch Kinder
*Thomas Schweiger*

## Warum die DSGVO in Drittländern umgesetzt werden sollte
*Tobias Tretzmüller*

## DSGVO: Löschen in Backups
*Thomas Schweiger*

## Warum Internet-Recherchen über Bewerber möglich sind
*Wolfram Hitz*

## Checkliste für Auftragsverarbeiter
*Rainer Knyrim*

dako.manz.at

ISSN 2313-5409

MANZ

Österreichische Post AG Info.Mail Entgelt bezahlt Retouren an Verlag Manz, Gutheil Schoder Gasse 17, 1230 Wien

Thomas Schweiger
Rechtsanwalt SMP Schweiger Mohr & Partner Rechtsanwälte OG

# Löschen in Backups – Anforderungen und rechtliche Möglichkeiten nach der DSGVO

**Das künftige EU-Datenschutzrecht – Teil 14.** Die Speicherbegrenzungen in zeitlicher Hinsicht rücken ins Interesse der Praktiker. Der OGH meint dazu: Löschen heißt Vernichten. Gibt es eine Möglichkeit, die (weitere) Verarbeitung von gelöschten personenbezogenen Daten in Datensicherungen zu rechtfertigen?

## Ausgangslage

Eine **Datensicherung** ist heute selbstverständlich und erfolgt in regelmäßigen Abständen. Von der Datensicherung ist die Archivierung von Daten, um zB steuerrechtlichen Aufbewahrungspflichten nachkommen zu können, zu unterscheiden. Eine „Backup-Richtlinie" mit Beschreibung der Sicherungsroutinen und Restore-Szenarien ist ebenso Stand der Technik. Mit den **Back-ups** (Datensicherungen) werden ua **Daten natürlicher Personen gespeichert**; diese **Verarbeitung kann in Widerspruch mit Datenminimierung, Speicherbegrenzung** und der **Verpflichtung zur Löschung** stehen.

**Art 17 Abs 1 DSGVO legt fest, dass personenbezogene Daten *„unverzüglich zu löschen [sind]"*,** wenn einer der in lit a bis f leg cit normierten Gründe vorliegt. Es stellt sich die Frage, ob die Daten nur im Aktivsystem zu löschen sind oder auch Datensicherungen von der Löschverpflichtung betroffen sind.

## Judikatur

Der OGH erachtet **Löschen im Archivsystem** als notwendig:[1] *„Allerdings kann das ‚Rechenzentrum' […] auf die ins Archiv gestellten personenbezogenen Daten […] weiterhin zugreifen, […] reicht […] Archivierung […] nicht aus, um der gesetzlichen Löschungsverpflichtung Rechnung zu tragen. [Wenn] Daten weiterhin – wenngleich einem eingeschränkten Kreis – vollinhaltlich zugänglich [sind, ist] eine ‚physische' Löschung der Daten erforderlich."* Ebenso urteilte der OGH:[2] *„Bereits […] verpflichtet […], die Daten physisch zu löschen, also so unkenntlich zu machen, dass eine Rekonstruktion nicht mehr möglich ist; eine Änderung der Datenorganisation dahingehend, dass ein gezielter Zugriff auf die betreffenden Daten ausgeschlossen ist, reicht hingegen nicht aus."*

## Literatur und DSB

Auch *Thiele*[3] führt aus: *„In seiner Löschungsanordnung verfestigt der OGH seine bisherige Rsp […] nicht genügt, die Datenorganisation so zu verändern, dass ein ‚gezielter Zugriff' auf die betreffenden Daten ausgeschlossen ist, um das Löschungsgebot […] zu erfüllen".*

Die Datenschutzbehörde[4] meint, dass „Löschen" nicht mit „Vernichten" gleichzusetzen ist: *„Nach dem allgemeinen Verständnis dieser Begriffe muss eine Löschung daher nicht zu einem sofortigen, endgültigen und unwiderruflichen Datenverlust führen. Es ist bei der Beurteilung einer Datenlöschung von einem durchschnittlichen Benutzer des in Rede stehenden Datenträgers auszugehen, der übliche Methoden der Datenabfrage bzw Informationsgewinnung zur Anwendung bringt. Für einen solchen Benutzer muss ein ‚Ausgeben' der Daten […] unmöglich sein. Keinesfalls aber muss eine gesetzmäßige Datenlöschung einer von einem Spezialisten mit wissenschaftlichen (forensischen) Methoden durchgeführten Suche nach Daten auf einem Datenträger standhalten."*

[1] OGH 11. 10. 2010, 6 Ob 112/10d. [2] Vgl OGH 13. 9. 2012, 6 Ob 107/12x. [3] Thiele, jusIT 2012/105, 227; OGH: Widerspruch gegen Wirtschaftsdatenbanken. [4] DSB K121.375/2008.

*Kastelitz/Leiter*[5] führen aus: *„Bedeutet ‚Löschen' jedoch nicht zwangsläufig vollständiges ‚Vernichten', wofür auch das DSG 2000 spricht, kennt dieses doch neben ‚Löschen' und ‚Sperren' explizit das ‚Vernichten'".*

### DSGVO

Die Definition von **„Verarbeitung"** in Art 4 Z 2 DSGVO unterscheidet zwischen **„Löschen"** und **„Vernichten"**, wobei keine inhaltliche Determinierung erfolgt. *Nolte/Werkmeister*[6] erwähnen, dass unter *„Löschen jedwede Art der Unkenntlichmachung erfasst"* sei. *Herbst*[7] äußert sich ebenfalls zum Löschen in Backups: *„Sofern der Verantwortliche über Sicherungskopien der zu löschenden Daten verfügt, sind auch die Sicherungskopien zu löschen".*

In einem **Entwurf** zu Art 17 DSGVO war in Abs 4 lit da vorgesehen, dass die Löschung dann nicht zu erfolgen hat, *„wenn die spezifische Art der Speichertechnologie keine Löschung ermöglicht und vor Inkrafttreten dieser Verordnung installiert wurde."* Diese Formulierung findet sich in der geltenden Fassung der DSGVO nicht (mehr). Das (novellierte) **DSG**[8] enthält zur Löschung eine an die bisherige Rechtslage des § 27 Abs 6 DSG 2000 angelehnte Ausführungsbestimmung: *„Kann die […] Löschung von automationsunterstützt verarbeiteten personenbezogenen Daten nicht unverzüglich erfolgen, weil diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann, so ist die Verarbeitung der betreffenden personenbezogenen Daten […] bis zu diesem Zeitpunkt einzuschränken."* Diese Bestimmung ermöglicht eine **zeitlich verzögerte Löschung der Daten**.[9]

### Grundlage für die Rechtmäßigkeit der Verarbeitung in Sicherungskopien

**Art 6 Abs 1 lit a bis f DSGVO** beschreibt die **Grundlagen der Rechtmäßigkeit** der Verarbeitung von personenbezogenen Daten; lit f erlaubt die Verarbeitung zur **Wahrung der berechtigten Interessen**, sofern die Interessen oder Grundrechte der betroffenen Personen nicht überwiegen. *„Zu den berechtigten Interessen des Verantwortlichen […] zählen nicht nur rechtliche, sondern auch tatsächliche, wirtschaftliche oder ideele Interessen."*[10]

ErwGr 49 DSGVO[11] verweist auf **IT-Sicherheit als berechtigtes Interesse**, sofern die Verarbeitung ausschließlich im Rahmen des notwendigen und für den Zweck angemessenen Umfangs erfolgt. Als Zweck wird die **Sicherstellung der Netzwerk- und Informationssicherheit** explizit genannt. Die *Breyer*-Entscheidung des EuGH[12] bestätigt, dass die *„Aufrechterhaltung der Sicherheit und Funktionsfähigkeit"* ein berechtigtes Interesse iZm einem IT-System ist.

Sicherungskopien werden aus Gründen der **Sicherheit in der Informationstechnologie** angefertigt. Das Österreichische Informationssicherheitshandbuch legt unter Pkt. 12.4 „Datensicherung" fest: *„Unabdingbare Voraussetzung für jeden Business Continuity Plan ist die Planung und Durchführung einer ordnungsgemäßen Datensicherung."*[13] Zur **Vermeidung von Datenverlusten** müssen regelmäßige Datensicherungen durchgeführt werden.[14] Art 4 Z 12 DSGVO[15] definiert ua den **Verlust von personenbezogenen Daten** als Verletzung der Sicherheit und damit Datenschutzverletzung. Daraus ist eindeutig ableitbar, dass Datensicherungen der IT-Sicherheit und auch dem Schutz vor Datenschutzverletzungen dienen.

Die Datensicherungen müssen in Bezug auf die gesicherten personenbezogenen Daten jedoch **„unbedingt notwendig und verhältnismäßig"**[16] sein, um ein berechtigtes Interesse darstellen zu können, und die Interessen und Grundrechte der natürlichen Personen dürfen nicht überwiegen.

## IT-Sicherheit ist ein berechtigtes Interesse für die Verarbeitung in Backups.

Eine Organisation, die das **„berechtigte Interesse"** als Grundlage für die Rechtmäßigkeit der weiteren Verarbeitung (Speicherung) personenbezogener Daten in Datensicherungen heranziehen möchte, muss ein angemessenes **Datensicherungskonzept** erarbeiten und in diesem Konzept beschreiben, wie die Sicherungen unter den maßgeblichen Faktoren (zB IT-System, Datenvolumen, Änderungsfrequenz der Daten und die Verfügbarkeitsanforderungen) tatsächlich erfolgen und wie mit den Datensicherungen umgegangen wird.

Daten werden nicht in lesbarer Form „kopiert" und „gesichert" (zB bestimmte Ordner auf eine externe Festplatte kopiert), sondern sie werden mit **speziellen Datensicherungsprogrammen** (untergliedert in konkrete Server, Clients, Datenarten oder Programme in periodischen Abständen) gesichert. Die Sicherung erfolgt meist in Form von Speicherabbildsicherungen. Es ist **nicht möglich**, dass **direkt aus dem aktiven Softwaresystem ohne notwendige Zwischenschritte** (Re-Storing der gesicherten Daten) auf die personenbezogenen Daten von den Personen, die bisher die Daten verarbeitet haben, zugegriffen werden kann.

## Ein Datensicherungskonzept ist Grundlage für die Rechtmäßigkeit der Speicherung.

Weitere Voraussetzungen sind:

- Nur ein eingeschränkter Personenkreis führt Datensicherungen durch.
- Auf die Backups, die räumlich getrennt von den Rechnern zu lagern sind, dürfen nur befugte Personen zugreifen.
- Die Personen, die die personenbezogenen Daten üblicherweise verarbeiten, haben auf die Backups keinen Zugriff.
- Eine genaue Festlegung des Re-Store-Ablaufes (mit Zugriffsberechtigungen und Prüfung des Datenbestandes) ist Bestandteil jedes Datensicherungskonzepts.
- Sicherungskopien erfolgen in regelmäßigen Abständen und die Sicherungskopien werden in periodischen Abständen überschrieben oder vernichtet und ha-

[5] *Kastelitz/Leiter*, jusIT 2010/69, 146; OGH: Art der Löschung nach Ausübung des Widerspruchsrechts. [6] *Nolte/Werkmeister* in Gola (Hrsg), Datenschutz-Grundverordnung, Art 17 DSGVO Rz 8. [7] *Herbst* in Kühling/Buchner, Datenschutz-Grundverordnung, Art 17 DSGVO Rz 42. [8] BGBl I 2017/120. [9] Arg „nicht unverzüglich", „nur zu bestimmten Zeitpunkten". ErläutRV 322/ME 25. GP 4: *Im DSG 2000 ist derzeit vorgesehen, dass dann, wenn die Löschung oder Richtigstellung von personenbezogenen Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern aus Gründen der Wirtschaftlichkeit nur zu bestimmten Zeitpunkten vorgenommen werden kann, die zu löschenden personenbezogenen Daten für den Zugriff zu sperren und die zu berichtigenden personenbezogenen Daten mit einer berichtigenden Anmerkung zu versehen sind (§ 27 Abs 6 DSG 2000). Die DSGVO trifft für einen solchen Fall keine ausdrückliche Vorsorge. Insbesondere bei einer etwa aus Sicherheitsgründen weit verteilten Speicherung von personenbezogenen Daten kann es sich im Einzelfall als schwierig erweisen, einzelne Datensätze sofort aus sämtlichen Kopien zu entfernen. In diesem Lichte erscheint die Beibehaltung einer technikneutral formulierten, adaptierten Fassung des bisherigen § 27 Abs 6 DSG 2000 sachgerecht.* [10] *Buchner/Petri* in Herbst, Datenschutz-Grundverordnung Art 6 Rz 146. [11] Der englische Text des ErwG 49 beschreibt das berechtigte Interesse der IT-Sicherheit eindeutiger als der deutsche Text: *The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping „denial of service" attacks and damage to computer and electronic communication systems.* [12] EuGH 19. 10. 2016, C-582/14, *Breyer/Deutschland*. [13] www.sicherheitshandbuch.gv.at/ [14] Siehe Pkt. 12.4.2. Österreichisches Informationssicherheitshandbuch. [15] „Verletzung des Schutzes personenbezogener Daten": eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. [16] Siehe ErwGr 49 DSGVO.

ben somit ein „Ablaufdatum". Die im Aktivsystem bereits gelöschten personenbezogenen Daten werden daher in periodischen Abständen gelöscht.

Aus rechtlicher Sicht werden die Sicherungskonzepte im Hinblick auf die **Aufbewahrungsdauer** uU zu überarbeiten sein, denn eine Aufbewahrung über einen Zeitraum von zwölf Monaten ist möglicherweise zu lange, wenn man bedenkt, dass das Interesse die Wiederherstellung möglichst aktueller Daten ist.

Bei der Löschung personenbezogener Daten ist es mE nicht notwendig, die Daten in der Sicherungskopie zu löschen, wenn ein eines angemessenes Datensicherungskonzept und dieses umgesetzt wird. Das „**berechtigte Interesse**" der **notwendigen und angemessenen Aufrechterhaltung der Informations- und Netzwerksicherheit** gestattet es, diese personenbezogenen Daten nach wie vor zu verarbeiten (zu speichern). Bei der Wiederherstellung von Daten aus der Sicherungskopie sind im Aktivsystem (vor der Wiederherstellung bereits) gelöschte Daten vor einer Zugriffsmöglichkeit (noch einmal) zu löschen, damit diese nicht in den aktiven Datenbestand übernommen werden.

Dako 2018/7

## Zum Thema

### Über den Autor

Dr. Thomas Schweiger, LL.M., CIPP/E, ist Rechtsanwalt und Partner der SMP Schweiger Mohr & Partner Rechtsanwälte OG.
E-Mail: office@dataprotect.at, Internet: www.dataprotect.at

### Link

Österreichisches Informationssicherheitshandbuch: www.informationssicherheitshandbuch.gv.at

### Hinweis

Dieser Beitrag ist der 14. Teil der Serie zum künftigen EU-Datenschutzrecht. Bisher erschienen sind:

- *Knyrim*, Die Datenschutz-Grundverordnung: Entwicklung und Anwendungsbereich, Dako 2015/21;
- *Pollirer*, Die Datenschutz-Grundverordnung: Der Datenschutzbeauftragte, Dako 2015/37;
- *Pollirer*, Die Datenschutz-Grundverordnung: Die Datenschutz-Folgenabschätzung, Dako 2015/47;
- *Wagner*, Die Datenschutz-Grundverordnung: Die Betroffenenrechte, Dako 2015/59;
- *Knyrim*, Die Datenschutz-Grundverordnung: Die neuen Pflichten, Dako 2016/6;
- *Leissler/Wolfbauer*, Die Datenschutz-Grundverordnung: Das „One-Stop-Shop"-Prinzip, Dako 2016/23;
- *Haidinger*, Geltendmachung der Betroffenenrechte und das Auskunftsrecht nach der Datenschutzgrundverordnung, Dako 2016/73;
- *Oman*, Die Handhabung von Datenpannen iSd DSGVO, Dako 2017/3;
- *Pilgermair*, Datenschutz-Grundverordnung: Der neue Kinderschutz, Dako 2017/4;
- *Schwaiger*, Die Datenschutz-Grundverordnung: Benötigt Ihr Unternehmen ab 25. 5. 2018 einen Datenschutzbeauftragten? Dako 2017/20;
- *Haidinger*, Datenschutz-Grundverordnung: Die Rechte auf Löschung, Berichtigung, Einschränkung und Datenübertragbarkeit, Dako 2017/34;
- *Haidinger*, Widerspruch, automatisierte Einzelentscheidungen und Informationspflichten nach der DSGVO, Dako 2017/63;
- *Hübelbauer*, DSGVO: Das Recht auf Datenübertragbarkeit, Dako 2017/64.