Umsetzung Datenschutz an der TBZ

1 Zweck

Datenschutzkonformes Handeln muss auch an der TBZ sichergestellt werden. In diesem Schulorganisationsblatt werden Klassifikation und entsprechende Handlungsanweisungen für die im Schulumfeld typischen Daten definiert.

2 Geltungsbereich

Datenschutzkonformes Handeln gilt für die gesamte TBZ.

3 Rechtliche Grundlage

- Bundesgesetz über den Datenschutz (DSG)
- Verordnung zum Bundesgesetz über den Datenschutz [VDSG]
- Gesetz über die Information und den Datenschutz (IDG) des Kantons Zürich

Der Datenschutzbeauftragter (DSB) des Kantons Zürich wirkt in einer beratenden und kontrollierenden Funktion.

4 Das Wichtigste in Kürze

Der Umgang mit Daten und Informationen, auf Papier oder elektronisch gespeichert, erfordert deren Klassifizierung. Im Schulumfeld verwenden wir folgende Klassifizierung:

- *„Öffentlich“* – Daten/Informationen für die Öffentlichkeit
- *„Intern“* - Schul-Interne Daten/Informationen wie z.B. Teilnoten oder Einzelnoten
- *„Vertraulich“* - Vertrauliche Daten/Informationen (Geheim) wie z.B. Gesamt- oder Zeugnisnoten

Vor jeder Speicherung oder Weitergabe von Daten ist diese Klassifizierung zu beachten und die in diesem Dokument beschriebenen Handlungsanweisungen anzuwenden.

Handlungsanweisungen am Beispiel von Schulnoten

Gesamt- oder Zeugnisnoten nur an Personen weitergeben, für die die Noten bestimmt sind. Digitale Weitergabe darf nur in verschlüsselter Form oder über eine sichere Plattform erfolgen. Die Speicherung darf nur auf sicheren Plattformen erfolgen, wie zur Zeit BSCW, Microsoft Office 365 mit OneDrive for Business, nicht aber DropBox, GoogleDocs.

Persönliche Teil- oder Einzelnoten dürfen nur mit Einverständnis des Betroffenen an andere Personen weitergeben werden.

5 Weiterführende Unterlagen und Links

Datenschutzbeauftragter (DSB), Kanton Zürich	https://dsb.zh.ch/internet/datenschutzbeauftragter/
Datenschutzbeauftragter (DSB), Kanton Zug	http://www.datenschutz-zug.ch/
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)	https://www.edoeb.admin.ch/
privatim, die Vereinigung der schweizerischen Datenschutzbeauftragten	http://www.privatim.ch/
ICT-Security Newsletter der TBZ	https://bscw.tbz.ch/bscw/bscw.cgi/21452425

6 Richtlinie

6.1 Klassifizierung der Daten

Für einen korrekten Umgang mit Daten müssen diese stets richtig klassifiziert werden. Anschliessend sind für den Umgang die der Klassifizierung entsprechenden Massnahmen zu beachten. Insbesondere für sensitive Daten, dies sind Daten wo Missbrauch und Schadenausmass erhöht sein kann, gelten besondere Massnahmen.

Ebenso ist das Öffentlichkeitsprinzip zu berücksichtigen, welches öffentlichen Organe zur Information über ihre Tätigkeit verpflichtet. An der TBZ geschieht dies im Verantwortungsbereich des Rektors.

Was sind nun „sensitive Daten“? Um dies zu verstehen und den Schutz dieser Daten in der täglichen Anwendung zu vereinfachen hilft die schulweite Einteilung von Daten in Klassifizierungsstufen. Folgende Klassifizierungsstufen sind für das Schulumfeld sinnvoll und anwendbar:

- *„Öffentlich“* – Daten/Informationen für die Öffentlichkeit
- *„Intern“* - Schul-Interne Daten/Informationen
- *„Vertraulich“* - Vertrauliche Daten/Informationen (Geheim)

Die Klassifizierung der Daten wird anhand deren Sensitivität vorgenommen. Die Sensitivität spiegelt die Empfindlichkeit der Daten auf Missbrauch oder das mögliche Schadensausmass.

Basierend auf diesen Klassifizierungen sind gewisse Verhaltensweisen nötig, um datenschutzkonform zu handeln und den Schutz der Daten zu gewährleisten.

6.2 Klassifizierung und Datentypen

„Öffentlich“ – Daten/Informationen für die Öffentlichkeit

Daten/Informationen werden als „öffentlich“ klassifiziert, falls sie zur Abgabe für die Öffentlichkeit, für die Medien, für Kunden, Partner oder Lieferanten erstellt wurden. Sie stehen allen Mitarbeitenden und Dritten frei zur Verfügung.

„Intern“ – Schul-Interne Daten/Informationen

Alle Daten/Informationen, die nicht für die allgemeine Öffentlichkeit bestimmt sind, die aber innerhalb der TBZ von den vorgesehenen Empfängern eingesehen werden dürfen, sind als „intern“ zu klassifizieren.

„Vertraulich“ - Vertrauliche Daten/Informationen

Daten/Informationen die aufgrund ihres Inhaltes nur spezifischen Benutzergruppen zugänglich sein dürfen, müssen als „vertraulich“ klassifiziert werden. Im Speziellen betrifft dies Personendaten.

Der Adressatenkreis darf nicht unautorisiert erweitert werden. Es gilt immer, das „need-to-know“-Prinzip zu befolgen, d.h. der Zugriff auf vertrauliche Informationen ist nur dann zu gewährleisten, wenn dies für die Erfüllung der Aufgabe notwendig ist. Die Weitergabe dieser Daten/Informationen muss zweckorientiert erfolgen.

6.3 Beispiele von Datentypen

Die untenstehende Tabelle zeigt allgemein und spezifisch im Schulumfeld existierende Dokumente. Diese Liste ist nicht als abschliessend zu betrachten.

„Öffentlich“ Daten/Informationen für die Öffentlichkeit	„Intern“ Schul-Interne Daten/Informationen	„Vertraulich“ Vertrauliche Daten/Informationen
Jahresbericht, Kursausschreibungen, Stundenpläne ohne Personenangaben, TBZ-Website, etc.	Teilnoten, Einzelprüfungen (idealerweise aber auch wie vertrauliche Daten behandeln) Korrespondenz und Gesuche (z.B. Parkgesuche, Dispensationsgesuche, Verschiebungsgesuche, Militär) Richtlinien, Arbeitsanweisungen Protokolle (ausser „vertrauliche“ Protokolle)	Schul-Zeugnisse, Noten QV-relevante Prüfungen und Arbeiten Prüfungsausweise Arztzeugnisse Disziplinarische Massnahmen Schülerakten (z.B. Arztzeugnisse, Dispensen, Situationsberichte …) Personalakten (Bewerbungen, Lohnausweise, Mitarbeiterbeurteilungen, Religion, Politische Aktivitäten, Aktennotizen, ...) Zugangsdaten (User-ID, Passwörter, Codes, PINs)
Medienmitteilungen und Medieninformationen Veröffentlichte Geschäfts-/Schulberichte Werbeinformationen (Broschüren, Inserate, Texte, Bilder, Video- und Audioaufnahmen) Öffentliche Informationen für Geschäftspartner und Kunden Allgemeine Geschäftsbedingungen	Organigramme Allgemeine Korrespondenz Weisungen, Richtlinien, Arbeitsanweisungen, Prozessbeschreibungen, Checklisten Sitzungsprotokolle (ausser „vertrauliche“ Sitzungs-protokolle)	Personenbezogene Daten gemäss Eidg. Datenschutz-gesetz (inkl. besonders schützenswerte Daten) Datensammlungen, die eine Beurteilung wesentlicher Aspekte einer Persönlichkeit einer Person erlauben (Persönlichkeitsprofile) Persönliche Mitarbeiterdaten (z.B. Mitarbeiterbeurteilungen, Lohndaten) Persönliche Informationen von Dritten (z.B. Bewerbungsunterlagen) Protokolle und geschäftsstrategische Daten der Schulleitung Vertragsunterlagen Revisionsberichte

6.4 Handlungsanweisungen

Für korrektes datenschutzkonformes Handeln sind an der TBZ die folgenden Handlungsanweisungen einzuhalten:

- Für die Daten der Klassifizierung „Öffentlich“ gibt es keine speziellen Handlungsanweisungen.
- Daten mit der Klassifizierung „Intern“ sollen nur Schulmitarbeitenden und/oder den Schülern (Kunden) zur Verfügung stehen, dies ohne weitere Restriktionen.
- Daten mit der Klassifizierung „Vertraulich“ haben einen erhöhten Schutzbedarf und müssen besonders geschützt werden.

	„Intern“ Schul-Interne Daten/Informationen	**„Vertraulich“** Vertrauliche Daten/Informationen
Generell		
Zugriffsrechte	Die Zugriffsrechte sind auf die TBZ Mitarbeitenden und/oder auf die Schüler (Kunden) einzuschränken.	Die Zugriffe auf diese Informationen sind strikt nach dem Prinzip „need-to-know“ auf ein Minimum zu begrenzen.
Auskunftsrecht	Gegen Extern: Keine Auskunft (ausser persönliche Daten oder Behörden)	Gegen Extern: Keine Auskunft (ausser persönliche Daten oder Behörden) Die Weitergabe und Freigabe ist nur zulässig, falls der Empfänger diese Daten zur Erfüllung seiner Aufgabe benötigt gemäss dem „need-to-know“-Prinzip und dazu berechtigt ist.
Speicherung		
Speichern auf mobilen, externen Datenträgern (z.B. USB Sticks, Mobile Phones)	Keine Einschränkung solange der Zugang auf die vorgesehenen Empfänger beschränkt bleibt. Eine Verschlüsselung der Daten ist jedoch empfohlen.	Datenspeicherung auf externen Speichermedien ist nicht bzw. nur in Ausnahmefällen und mit einer anschliessenden möglichst schnellen sofortigen Löschung zulässig. Dabei sind Daten zu verschlüsseln. Es sind nur Kopien der Originaldaten zu speichern.
Laufwerke auf Schulinfrastruktur (Shared Drives)	Keine Einschränkung solange der Zugang auf die vorgesehenen Empfänger beschränkt bleibt.	Zugriffseinschränkung auf Folder/Verzeichnis mit explizitem Zugriffsschutz auf Basis des „need-to-know“ Prinzipes.
Cloud Speicherlösungen, durch Schule empfohlen	Keine Einschränkung solange der Zugang auf die vorgesehenen Empfänger beschränkt bleibt.	Zugriffseinschränkung auf Folder/Verzeichnis mit explizitem Zugriffsschutz auf Basis des „need-to-know“ Prinzipes.

Cloud Speicherlösungen, nicht durch Schule empfohlen (z.B. Dropbox, GoogleDrive)	Keine Speicherung empfohlen	Keine Speicherung erlaubt
Kollaborationsplattformen, durch Schule empfohlen (z.B. BSCW, Microsoft Office 365 mit OneDrive for Business, ecolm)	Keine Einschränkung solange der Zugang auf die vorgesehenen Empfänger beschränkt bleibt.	Zugriffseinschränkung auf Folder/Verzeichnis mit explizitem Zugriffsschutz auf Basis des „need-to-know“ Prinzipes
Kollaborationsplattformen, nicht durch Schule empfohlen (z.B. GoogleDocs, Moodle)	Keine Speicherung empfohlen	Keine Speicherung
Social Media und andere Online-Plattformen	Keine Speicherung	Keine Speicherung
Kommunikation		
Kommunikation, Daten-Übermittlung, durch Schule empfohlen (z.B. TBZ E-Mail Plattform, WebTransfer ZH)	Keine Einschränkung solange der Zugang auf die vorgesehenen Empfänger beschränkt bleibt. Versand auf TBZ E-Mail Adressen beschränken.	Eingeschränkt – Daten dürfen nur an Empfänger übermittelt werden, die diese Daten zur Erfüllung ihrer Aufgabe benötigen gemäss dem „need-to-know“-Prinzip und dazu berechtigt sind. Falls es sich dabei um Dritte handelt, sind vorgängig Vertraulichkeitsvereinbarungen zu unterzeichnen. Daten müssen bei der elektronischen Übermittlung nach Extern verschlüsselt sein.
Kommunikation, Daten-Übermittlung, durch Schule nicht empfohlen (z.B. WeTransfer)	Keine Benutzung empfohlen	Keine Benutzung erlaubt
Physische Dokumente		
Ablage	Keine Einschränkung solange der Zugang auf die vorgesehenen Empfänger beschränkt bleibt.	Physische Dokumente müssen unter Verschluss gehalten werden.
Kopieren / Drucken	Keine Einschränkung solange der Zugang auf die vorgesehenen Empfänger beschränkt bleibt.	Persönlich kopieren, nicht unbeaufsichtigt liegen lassen, sofort entfernen Nur mit Follow-Me-Printing ausdrucken, sofort und persönlich abholen und nicht liegen lassen

Entsorgung/ Vernichtung	Interne Entsorgung	Vertrauliche Daten in Papierform müssen mittels Aktenvernichter oder durch Entsorgungsfirma vernichtet werden. Daten auf Digitalen Datenträger sind unwiderruflich zu löschen (sog. „Wipen“).
Postversand	Keine Einschränkung solange der Zugang auf die vorgesehenen Empfänger beschränkt bleibt.	Sendungen mit besonders schützenswerten Daten müssen mit PERSÖNLICH oder VERTRAULICH (Stellvertreter darf öffnen) und dem Namen des Empfängers gekennzeichnet sein.

Handlungsanweisung 1: Wie sollen Noten kommuniziert werden?

„Intern“	Teilnoten, Einzelnoten, Einzelergebnisse
	Im Sinne eines einheitlichen Umganges mit Noten ist es sinnvoll alle Noten gleich zu behandeln, d.h. als „vertraulich“ zu behandeln. Dies wäre aber in der Umsetzung wohl nicht praktikabel. Um die Schule und die Lehrer vor möglichen Klagen zu schützen und die Privatsphäre der Schüler zu gewährleisten ist es notwendig vor der öffentlichen Bekanntgabe von persönlichen Noten **das Einverständnis jedes Betroffenen einzuholen** (sei dies schriftlich oder mündlich).

„Vertraulich“	Gesamt-Noten (z.B. Modulnoten), Zeugnisnoten, Notenübersichten, Noten- und Bewertungsdurchschnitte
	Diese Daten sind schützenswert. Deshalb muss die Speicherung und Weitergabe auch entsprechend erfolgen. D.h. die Weitergabe (mündlich, schriftlich, digital) darf nur an die Personen erfolgen, für die die Noten bestimmt sind. Die Daten sind dabei so zu schützen (u.a. Zugriffskontrolle), dass es keinem Dritten möglich ist die Daten einzusehen. Die Übermittlung mittels Email muss verschlüsselt erfolgen oder die Daten werden über ein Portal ausgetauscht, welches einen sicheren Umgang bietet (z.B. Microsoft Office 365 mit OneDrive for Business oder BSCW).

Handlungsanweisung 2: Wie sollen grosse und als „vertraulich“-klassifizierten Datenmengen mit Externen ausgetauscht werden?

Grosse Datenmengen können über ein gesichertes Portal wie beispielsweise BSCW und OneDrive for Business ausgetauscht werden. Ebenfalls stellt der Kanton Zürich dazu den Dienst WebTransfer ZH zur Verfügung.

Verfasser: ICT-Security-Team der TBZ, Beat Hartmann, 31. August 2017

Genehmigt: SLS vom 9. Sept. 2017