Klasse: Arbeitsblatt
Name: DSGVO
Datum: LF7b 21.01.2021

ab) Für die Formulierung einer Datenschutzrichtlinie für die Fidule GmbH sollen Sie die Rechte der Betroffenen laut Datenschutzgrundverordnung (DSGVO) ermitteln. Datenschutz-Grundverordnung

Nennen Sie davon vier Rechte. 4 Punkte

1. Recht auf Berichtigung [Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen.]
2. Recht auf Löschung [Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden]
3. Auskunftsrecht [Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden]
4. Widerspruchsrecht [Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen]

b) Sie haben die Risikoanalyse durchgeführt, bei der folgenden Fälle aufgetreten sind. Bezeichnen Sie für jeden Fall das Risiko und schlagen Sie eine geeignete Abwehrmaßnahme vor.

ba) Ein Mitarbeiter verändert in der Datenbank das Rechnungsdatum mehrerer bereits gezahlter Kundenrechnungen, um in einer Besprechung ein besseres Umsatzergebnis für das dritte Quartal präsentieren zu können. 2 Punkte

Bezeichnung des Risikos:

ungewollte Datenmanipulation

Abwehrmaßnahme:

Datenbank gegen Unbefugte sichern (Kennwort)
Protokoll führen
Formatsbeschränkung

bb) Eine nicht im Verkauf beschäftigte Person setzt sich ohne generelle Erlaubnis an einen freien PC-Arbeitsplatz in der Verkaufsabteilung und lässt sich Statistiken zu Bestellungen anzeigen. 2 Punkte

Bezeichnung des Risikos:

unberechtigter Datenzugriff

Abwehrmaßnahme:

PC-Arbeitsplatz bei Verlassen sperren (Kennwort-Schutz)
Zugriffskontrollen/Zugangskontrollen (örtlich)

bc) Die Sicherungsbänder werden im selben Raum aufbewahrt, in dem das Datensicherungsgerät steht. Durch einen Brand im Raum werden die Festplatten und die Sicherungsbänder, auf denen alle Rechnungsdaten gespeichert sind, völlig zerstört. 2 Punkte

Bezeichnung des Risikos:

ungewollter Datenverlust
physischer Datenverlust

Abwehrmaßnahme:

Sicherungen räumlich getrennt aufbewahren
gegen Feuer schützen (Brandschutzanlage)

Die Fidule GmbH will das B2B-Bestellverfahren absichern.

Erläutern Sie die folgenden Schutzziele:

ca) Integrität (Manipulation muss nachvollziehbar sein) 2 Punkte

Allgemein gesehen bedeutet der Begriff Integrität, dass jemand glaubwürdig ist. Weitere Bedeutungen sind Ehrlichkeit, Anständigkeit, Makellosigkeit, Rechtschaffenheit oder auch Unbestechlichkeit. OK, dabei denkt man wohl eher an eine Person. Zurück zu personenbezogenen Daten und dem Datenschutz. Stellen Sie sich vor, diese Eigenschaften könnten auch Dateneigenschaften beschreiben. Jetzt helfen Ihnen die Begriffe hoffentlich bei der Einordnung und dem Verständnis etwas weiter. Wir sprechen von glaubwürdigen und unverfälschten Daten. Integre Daten sind echte Daten, oder Daten von denen die Echtheit nachvollziehbar ist. Aus der Integrität ergibt sich im Datenschutz eine enge Verbundenheit mit der Vertraulichkeit – einem anderen Schutzziel im Datenschutz. Denn nur wenn Sie sicherstellen, dass Daten nicht unberechtigt verändert werden, verfügen Sie über echte unverfälschte Daten. Sie sehen, das eine greift ins andere.

Klasse: Arbeitsblatt
Name: DSGVO Datum:

Aussage	Ziffer
Die Richtigkeit der Datenverarbeitung muss gewährleistet sein und es besteht ein Aktualisierungsanspruch bei Fehlern	5
Die Zwecke der Datenverarbeitung müssen bereits bei der Erhebung festgelegt, eindeutig und legitim sein.	3
Die verantwortliche Stelle muss jederzeit umfassende Informationen an die betroffenen Personen geben können, welche Daten durch wen und zu welchen Zwecken verarbeitet werden und wurden.	2
Dem Zweck angemessen und auf das notwendige Maß beschränkt.	4
Die Verarbeitung der Daten beruht auf Einwilligung der betroffenen Person.	1
Die Speicherung von Daten unterliegt einer zeitlichen Begrenzung.	6
Der Schutz personenbezogener Daten vor unerlaubtem Zugriff und Veränderung muss durch technische und organisatorische Maßnahmen sichergestellt sein. – Datenschutz durch Technik, datenschutzfreundliche Voreinstellungen, Zertifizierungsverfahren und Datenschutzsiegel.	7

1. Rechtmäßigkeit
2. Transparenz
3. Zweckbindung
4. Datenminimierung
5. Richtigkeit
6. Speicherbegrenzung
7. Integrität und Vertraulichkeit

In der Teamsitzung spricht der Datenschutzbeauftragte die Themen „Privacy by Design" und „Privacy by Default" an. Beide beinhalten Anforderungen, um Datenschutzgrundsätze zu implementieren – sowohl durch technische als auch organisatorische Maßnahmen.
Privacy by Design verlangt, Datenschutzprobleme schon bei der Entwicklung neuer Technologien festzustellen und zu prüfen, sodass der Datenschutz von Vornherein in die Gesamtkonzeption einbezogen wird.
Privacy by Default verlangt, dass Produkte oder Dienstleistungen standardmäßig datenschutzfreundlich konfiguriert sind.

Ergänzen Sie die Tabelle um weitere drei technisch-organisatorische Maßnahmen (TOM) zum Schutz personenbezogener Daten, die diesen Prinzipien genügen. 6 Punkte

	Technisch organisatorische Maßnahme
Beispiel	Menge der personenbezogene Daten minimieren
1	1. Pseudonymisierung Wikipedia definiert die Pseudonymisierung als einen Vorgang, bei dem persönliche Daten durch z.B. Zahlenfolgen ersetzt werden, so dass diese nicht mehr zuordenbar sind. Also z.B. Ersetzung einer E-Mail Adresse durch eine User-ID.
	2. Verschlüsselung Hier geht es um den Schutz der Daten vor unberechtigten Zugang z.B. durch Passwörter auf Archiven.
	3. Gewährleistung der Vertraulichkeit Hier geht es um alles, was mit Zutritt und Zugang zu tun hat, wie gewährleisten Sie, dass nur Berechtigte Zugang zum Serverraum haben?