Maßnahmenbericht zu Standard/Norm

EU-Datenschutzgrundverordnung

Inhaltsverzeichis

DSGVO
EU-Datenschutzgrundverordnung 1

01 Kap. I Allgemeine Bestimmungen 2

Art. 01 Gegenstand und Ziele 2
Art. 02 Sachlicher Anwendungsbereich 2
Art. 03 Räumlicher Anwendungsbereich 2
Art. 04 Begriffsbestimmungen 2

02 Kap. II Grundsätze 3

Art. 05 Grundsätze für die Verarbeitung personenbezogener Daten 3
Art. 05 Abs. 1 Grundsätze für die Verarbeitung personenbezogener Daten 3
Art. 05 Abs. 1 lit. a "Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz" 3
Art. 05 Abs. 1 lit. b "Zweckbindung" 6
Art. 05 Abs. 1 lit. c "Datenminimierung" 6
Art. 05 Abs. 1 lit. d "Richtigkeit" 6
Art. 05 Abs. 1 lit. e "Speicherbegrenzung" 6
Art. 05 Abs. 1 lit. f "Integrität und Vertraulichkeit" 7
Art. 05 Abs. 2 "Rechenschaftspflicht" 7
Art. 06 Rechtmäßigkeit der Verabeitung 7
Art. 06 Abs. 01 Rechtmäßigkeit 7
Art. 06 Abs. 1 lit. a Einwilligung 7
Art. 06 Abs. 1 lit. b Vertragserfüllung / vorvertragliche Verpflichtungen 7
Art. 06 Abs. 1 lit. c gesetzliche Verpflichtungen 8
Art. 06 Abs. 1 lit. d lebenswichtige Interessen 8
Art. 06 Abs. 1 lit. e öffentliche Interessen 8
Art. 06 Abs. 1 lit. f berechtigte Interessen des Verantwortlichen / eines Dritten 8
Art. 06 Abs. 02 Anpassung durch die Mitgliedsstaaten 8
Art. 06 Abs. 03 Festlegung der Rechtsgrundlage 8
Art. 06 Abs. 04 Zweckänderung 8
Art. 07 Bedingungen für die Einwilligung 8
Art. 08 Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft 8
Art. 09 Verarbeitung beonderer Kategorien personenbezogener Daten 8
Art. 09 Abs. 1 Definition 8
Art. 09 Abs. 2 Erlaubnistatbestand 8
Art. 09 Abs. 2 lit. a Einwilligung 8
Art. 09 Abs. 2 lit. b Arbeitsrecht und soziale Sicherheit 8
Art. 09 Abs. 2 lit. c lebenswichtige Interessen 8
Art. 09 Abs. 2 lit. d Mitgliederverwaltung von Kirchen, Gewerkschaften, etc. 8

Inhaltsverzeichis

Art. 09 Abs. 2 lit. e selbst öffentlich gemacht 9
Art. 09 Abs. 2 lit. f Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen 9
Art. 09 Abs. 2 lit. g erhebliches öffentliches Interesse 9
Art. 09 Abs. 2 lit. h Gesundheitsvorsorge 9
Art. 09 Abs. 2 lit. i öffentliche Gesundheit 9
Art. 09 Abs. 2 lit. j Archivzwecke, wissenschaftliche und historische Forschung 9
Art. 09 Abs. 3 Standesrecht für Gesundheitsberufe / Berufsgeheimnis 9
Art. 09 Abs. 4 weitere Einschränkungen 9
Art. 10 Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten 9
Art. 11 Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist 9

03 Kap. III Rechte der betroffenen Person 10

Abschnitt 1 Transparenz und Modalitäten 10
Art. 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person 11
Abschnitt 2 Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten 15
Art. 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person 15
Art. 14 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden 18
Art. 15 Auskunftsrecht der betroffenen Person 21
Abschnitt 3 Berichtigung und Löschung 22
Art. 16 Recht auf Berichtigung 22
Art. 17 Recht auf Löschung („Recht auf Vergessenwerden“) 23
Art. 18 Recht auf Einschränkung der Verarbeitung 23
Art. 19 Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung 24
Art. 20 Recht auf Datenübertragbarkeit 24
Abschnitt 4 Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall 24
Art. 21 Widerspruchsrecht 25
Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling 25
Art. 22 Abs. 1 Verbot der automatisierten Entscheidung im Einzelfall 25
Art. 22 Abs. 2 Erlaubnistatbestand für automatisierte Entscheidungen im Einzelfall 25
Art. 22 Abs. 2 lit. a Vertragsabschluss / Vertragserfüllung
Art. 22 Abs. 2 lit. b Rechtsvorschriften
Art. 22 Abs. 2 lit. c ausdrückliche Einwilligung
Art. 22 Abs. 3 angemessene Maßnahmen 25
Art. 22 Abs. 4 Entscheidungen auf Basis besonderer Kategorien personenbezogener Daten 25

Inhaltsverzeichis

Abschnitt 5 Beschränkungen 25

Art. 23 Beschränkungen 25

04 Kap. IV Verantwortlicher und Auftragsverarbeiter 26

Abschnitt 1 Allgemeine Pflichten 26

Art. 24 Verantwortung des für die Verarbeitung Verantwortlichen 26

Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen 28

Art. 25 Abs. 1 Privacy by Design 28

Art. 25 Abs. 2 Privacy by Default 28

Art. 26 Gemeinsam für die Verarbeitung Verantwortliche 28

Art. 26 Abs. 1 Vereinbarung 28

Art. 26 Abs. 2 Funktionen und Beziehungen 28

Art. 26 Abs. 3 Geltendmachung von Rechten 29

Art. 27 Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern 29

Art. 28 Auftragsverarbeiter 29

Art. 29 Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters 29

Art. 30 Verzeichnis von Verarbeitungstätigkeiten 29

Art. 31 Zusammenarbeit mit der Aufsichtsbehörde 29

Abschnitt 2 Sicherheit personenbezogener Daten 29

Art. 32 Sicherheit der Verarbeitung 29

Art. 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde 29

Art. 34 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person 29

Abschnitt 3 Datenschutz-Folgenabschätzung und vorherige Konsultation 29

Art. 35 Datenschutz-Folgenabschätzung 29

Art. 36 Vorherige Konsultation 30

Abschnitt 4 Datenschutzbeauftragter 30

Art. 37 Benennung eines Datenschutzbeauftragten 30

Art. 38 Stellung des Datenschutzbeauftragten 30

Art. 39 Aufgaben des Datenschutzbeauftragten 30

Abschnitt 5 Verhaltensregeln und Zertifizierung 30

Art. 40 Verhaltensregeln 30

Art. 41 Überwachung der genehmigten Verhaltensregeln 30

Art. 42 Zertifizierung 30

Art. 43 Zertifizierungsstellen 30

05 Kap. V Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen 31

Inhaltsverzeichis

Art. 44 Allgemeine Grundsätze der Datenübermittlung 31
Art. 45 Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses 31
Art. 46 Datenübermittlung vorbehaltlich geeigneter Garantien 32
Art. 47 Verbindliche interne Datenschutzvorschriften 32
Art. 48 Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung 32
Art. 49 Ausnahmen für bestimmte Fälle 32
Art. 50 Internationale Zusammenarbeit zum Schutz personenbezogener Daten 33

06 Kap. VI Unabhängige Aufsichtsbehörden 34

Art. 51 Aufsichtsbehörde 34
Art. 52 Unabhängigkeit 34
Art. 53 Allgemeine Bedingungen für die Mitglieder der Aufsichtsbehörde 34
Art. 54 Errichtung der Aufsichtsbehörde 34
Art. 55 Zuständigkeit 34
Art. 56 Zuständigkeit der federführenden Aufsichtsbehörde 34
Art. 57 Aufgaben 34
Art. 58 Befugnisse 34
Art. 59 Tätigkeitsbericht 34

07 Kap. VII Zusammenarbeit und Kohärenz 35

Art. 60 Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den anderen betroffenen Aufsichtsbehörden 35
Art. 61 Gegenseitige Amtshilfe 35
Art. 62 Gemeinsame Maßnahmen der Aufsichtsbehörden 35
Art. 63 Kohärenzverfahren 35
Art. 64 Stellungnahme Ausschusses 35
Art. 65 Streitbeilegung durch den Ausschuss 35
Art. 66 Dringlichkeitsverfahren 35
Art. 67 Informationsaustausch 35
Art. 68 Europäischer Datenschutzausschuss 35
Art. 69 Unabhängigkeit 35
Art. 70 Aufgaben des Ausschusses 35
Art. 71 Berichterstattung 35
Art. 72 Verfahrensweise 35
Art. 73 Vorsitz 35

Inhaltsverzeichis

Art. 74 Aufgaben des Vorsitzes 35

Art. 75 Sekretariat 35

Art. 76 Vertraulichkeit 36

08 Kap. VIII Rechtsbehelfe, Haftung und Sanktionen 37

Art. 77 Recht auf Beschwerde bei einer Aufsichtsbehörde 37

Art. 78 Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde 37

Art. 79 Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter 37

Art. 80 Vertretung von betroffenen Personen 37

Art. 81 Aussetzung des Verfahrens 37

Art. 82 Haftung und Recht auf Schadenersatz 38

Art. 83 Allgemeine Bedingungen für die Verhängung von Geldbußen 38

Art. 84 Sanktionen 38

09 Kap. IX Vorschriften für besondere Verarbeitungssituationen 39

Art. 85 Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit 39

Art. 86 Verarbeitung und Zugang der Öffentlichkeit zu amtlichen Dokumenten 39

Art. 87 Verarbeitung der nationalen Kennziffer 39

Art. 88 Datenverarbeitung im Beschäftigungskontext 39

Art. 89 Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken 39

Art. 90 Geheimhaltungspflichten 39

Art. 91 Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften 39

10 Kap. X Delegierte Rechtsakte und Durchführungsrechtakte 40

Art. 92 Ausübung der Befugnisübertragung 40

Art. 93 Ausschussverfahren 40

11 Kap. XI Schlussbestimmungen 41

Art. 94 Aufhebung der Richtlinie 95/46/EG 41

Art. 95 Verhältnis zur Richtlinie 2002/58/EG 41

Art. 96 Verhältnis zu bereits geschlossenen Übereinkünften 41

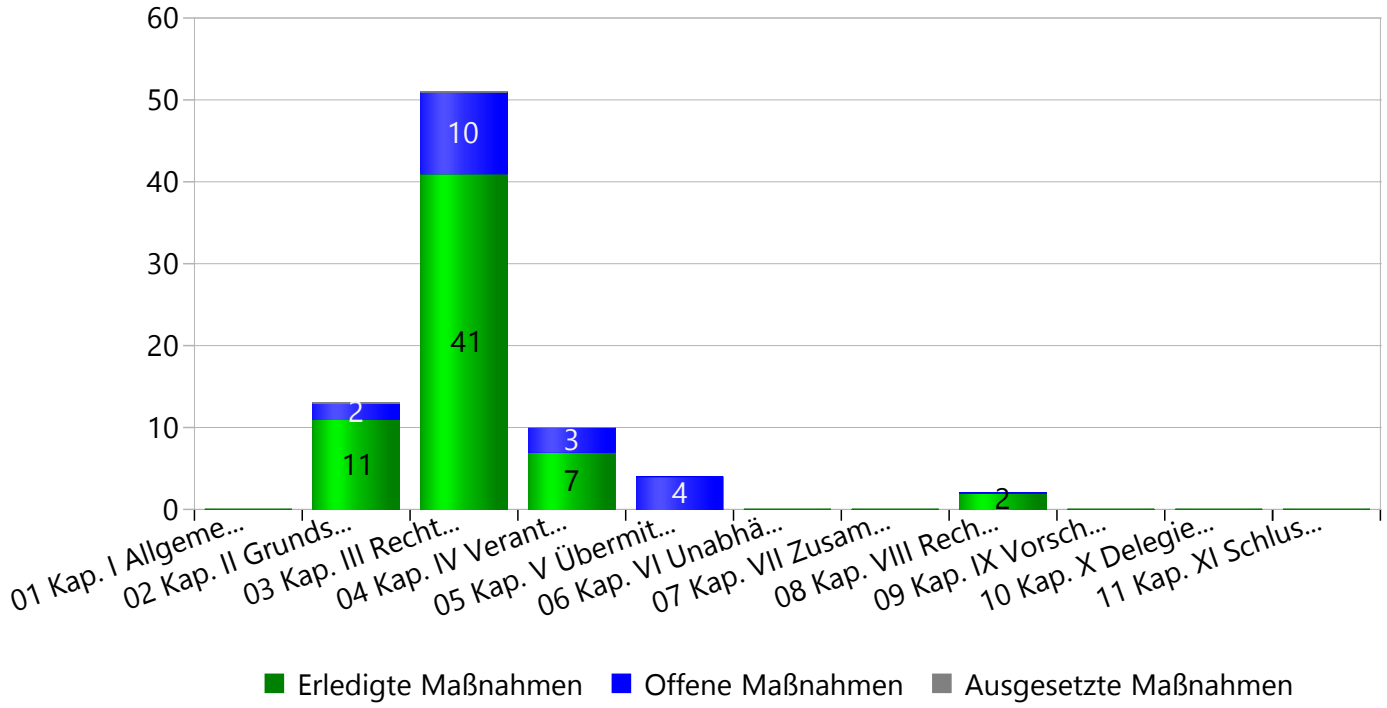
Inhaltsverzeichis

Art. 97 Berichte der Kommission	41
Art. 98 Überprüfung anderer Rechtsakte der Union zum Datenschutz	41
Art. 99 Inkrafttreten und Anwendung	41

DSGVO

EU-Datenschutzgrundverordnung

Stand:	25.05.2018
Beschreibung:	Gegenstand und Ziele der DSGVO (gemäß Art 1 der Verordnung) 1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten. 2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten. 3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.



01 Kap. I Allgemeine Bestimmungen

Art. 01 Gegenstand und Ziele

Keine zugewiesenen Maßnahmen

Art. 02 Sachlicher Anwendungsbereich

Keine zugewiesenen Maßnahmen

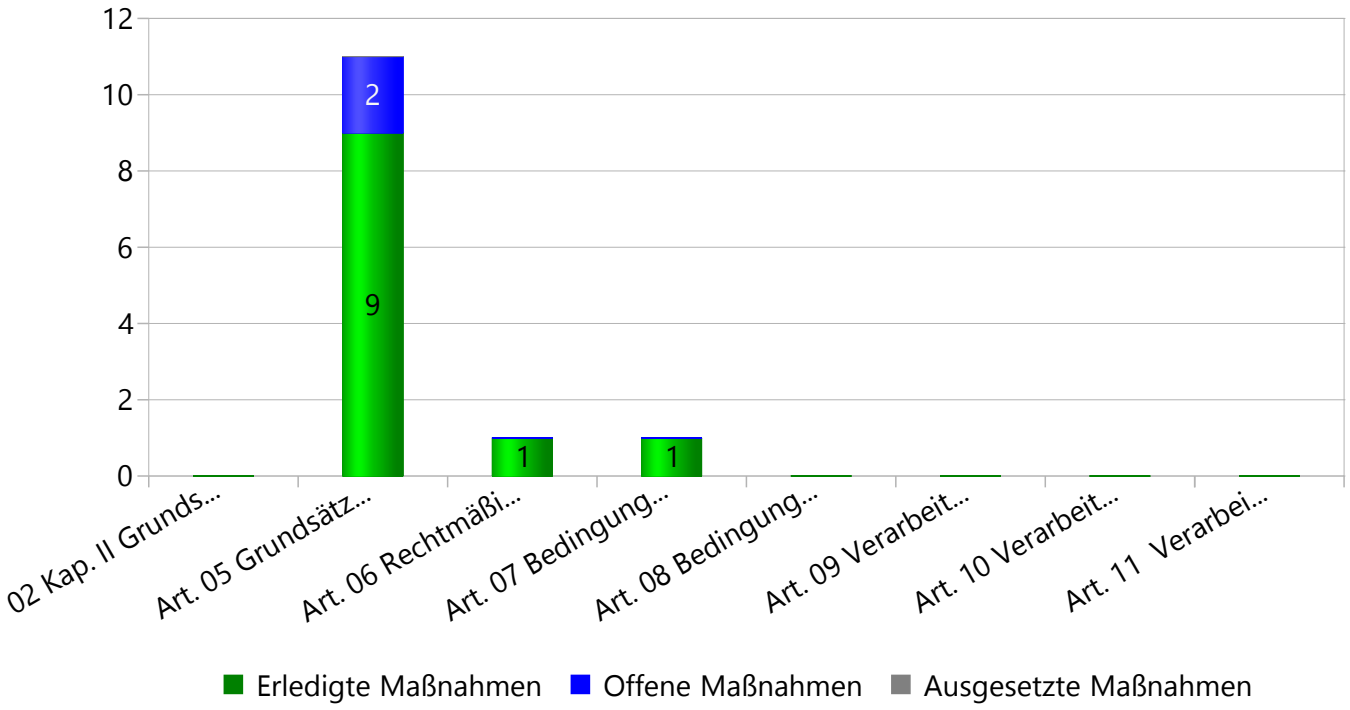
Art. 03 Räumlicher Anwendungsbereich

Keine zugewiesenen Maßnahmen

Art. 04 Begriffsbestimmungen

Keine zugewiesenen Maßnahmen

02 Kap. II Grundsätze



Art. 05 Grundsätze für die Verarbeitung personenbezogener Daten

Art. 05 Abs. 1 Grundsätze für die Verarbeitung personenbezogener Daten

Art. 05 Abs. 1 lit. a "Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz"

Offene Maßnahmen:

Maßnahme:	**M_DSMS_033 Zugang zur Datenschutzerklärung für Bewerber schaffen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Bewerber sollten im Zuge ihrer Bewerbung eine Datenschutzerklärung zur Verarbeitung ihrer personenbezogenen Daten erhalten. Es empfiehlt sich eine solche auf der Homepage einzubinden. Wenn die Möglichkeit einer Online-Bewerbung besteht bzw. Stellen online ausgeschrieben werden, sollte auf die relevante Datenschutzerklärung verlinkt werden.
Fortschritt:	0%

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_009 Rechtsgrundlage für Verarbeitungstätigkeiten überprüfen und dokumentieren**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Überprüfen Sie für jede von Ihnen durchgeführte Verarbeitungstätigkeit, ob eine gültige Rechtsgrundlage besteht. Die gängigsten Bedingungen für eine rechtmäßige Verarbeitung sind : - die Einwilligung der betroffenen Person - die Vertragserfüllung bzw. die Durchführung vorvertraglicher Maßnahmen - die Erfüllung einer rechtlichen Verpflichtung Dokumentieren Sie die Rechtsgrundlage für jede Verarbeitungstätigkeit (zB direkt im Verzeichnis von Verarbeitungstätigkeiten).
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	erledigt- siehe VVT

Maßnahme:	**M_DSMS_010 DSGVO-konforme Datenschutzerklärung erstellen**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Stellen Sie sicher, dass Ihre Datenschutzerklärungen alle geforderten Informationen enthalten. Dazu gehören grundsätzlich: - Namen und Kontaktdaten des Verantwortlichen (ggf. seines Vertreters) - Kontaktdaten des Datenschutzbeauftragten, wenn im Unternehmen einer bestellt ist - die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen - die Rechtsgrundlage für die Verarbeitung (insbesondere ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben ist oder für einen Vertragsabschluss erforderlich ist und ob die betroffene Person zur Bereitstellung der Daten verpflichtet ist und welche Folgen eine Nichtbereitstellung hätte Art 13 Abs 2 lit e) - die berechtigten Interessen des Verantwortlichen bzw. eines Dritten, wenn die Verarbeitung auf solchen beruht - die Empfänger oder Empfängerkategorien der personenbezogenen Daten, wenn personenbezogene Daten solchen offengelegt werden - die Übermittlung der personenbezogenen Daten an ein Drittland oder eine internationale Organisation, wenn eine solche geplant ist, sowie die Rechtsgrundlage einer solchen Übermittlung - die Speicherdauer der personenbezogenen Daten oder, wenn keine genaue Frist angegeben werden kann, zumindest die Kriterien für die Festlegung der Dauer - ein Hinweis auf die Möglichkeit der Ausübung der Rechte auf Auskunft, Löschung, Berichtigung, Widerspruch, Einschränkung und Datenübertragbarkeit - ein Hinweis darauf, dass erteilte Einwilligungen jederzeit widerrufen werden können, jedoch die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung davon nicht berührt wird - ein Hinweis auf das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde - aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und Auswirkungen für den Betroffen, wenn eine automatisierte Entscheidungsfindung besteht - maßgebliche Informationen im Zuge einer Zweckänderung bei der Weiterverarbeitung der personenbezogenen Daten Beachten Sie, dass Sie Betroffene auch über die Herkunft der Daten informieren müssen, falls diese nicht direkt bei der betroffenen Person erhoben wurden. Diese Informationen sind dann nicht zu erteilen, wenn die betroffene Person bereits über die Informationen verfügt.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	erledigt

Maßnahme:	**M_DSMS_011 Datenschutzerklärung auf Homepage einbinden**
OrgEH:	IT Abteilung TeSA (TeSA_IT)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Die Datenschutzerklärung muss auf der Homepage leicht auffindbar sein. Dazu muss die Datenschutzerklärung über einen eigenen Link von jeder Seite aus erreichbar sein. Stellen Sie im Zuge dessen auch sicher, dass alle Verarbeitungen, die im Zuge der Bereitstellung Ihrer Homepage getätigt werden, in der Datenschutzerklärung angeführt sind. Denken Sie dabei insbesondere an - den Einsatz von Cookies, Analyse- und Remarketingtools (zB Google Analytics, Google Adwords, etc - Daten, die Sie im Zuge von Kontaktformularen, Newslettern oder Blogs verarbeiten - die Verwendung von Social-Media Plugins - etwaige Chatfunktionen -...
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	erledigt

Maßnahme:	**M_DSMS_022 Datenschutzerklärung in Social-Media-Kanäle einbinden**
OrgEH:	IT Abteilung TeSA (TeSA_IT)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Wenn sich das Unternehmen auf Social-Media-Kanälen repräsentiert, sollte auch dort eine entsprechende Datenschutzerklärung vorgehalten werden. Dies betrifft insbesondere Facebook (siehe EuGH-Urteil ECLI "EU:C:2018:388"), kann aber auch auf andere Werbekanäle wie Instagram, Twitter, etc. umgemünzt werden. Die Auswirkungen dieses Urteils auf die Praxis sind noch offen. Es empfiehlt sich aber jedenfalls eine Datenschutzerklärung auf diesen Werbekanälen zu integrieren. Es kann dabei beispielsweise so vorgegangen werden: Bei Facebook kann zB unter "Info" ein Link zur Datenschutzerklärung untergebracht werden. Dabei sollte in der Datenschutzerklärung auf die Zwecke und den Umfang der Facebook-Nutzung durch das Unternehmen hingewiesen werden. Für die Nutzung der Daten durch Facebook kann auf die Datenrichtlinie von Facebook verwiesen werden.
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	Datenschutzerklärung ist in allen Kanälen integriert

Maßnahme:	**M_DSMS_023 Zugang zur Datenschutzerklärung für Mitarbeiter schaffen**
OrgEH:	Personalabteilung TeSA (TeSA_PER)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Mitarbeiter sollten im Zuge der Einstellung und der regelmäßigen Datenschutz-Schulung über die Verarbeitung sie betreffender personenbezogener Daten informiert werden und in weiterer Folge Zugriff zur für sie relevanten Datenschutzerklärung haben. Dies kann zB durch Aushändigen einer Kopie oder Verweis auf ein Dokument in einem jederzeit zugänglichen Ordner (online/offline) oder durch Zugriff über ein Intranet erfolgen.
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	an alle kommunziert und am Z-Laufwerk jederzeit abrufbar

Art. 05 Abs. 1 lit. b "Zweckbindung"

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_006 gesetzliche Aufbewahrungspflichten überprüfen**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Überprüfen Sie für jede Verarbeitungstätigkeit, ob es für die personenbezogenen Daten gesetzliche Aufbewahrungspflichten gibt, die einer frühzeitigen Löschung dieser Daten entegegenstehen. Überprüfen Sie des Weiteren, ob es gesetzliche Verpflichtungen gibt, für die gewisse personenbezogene Daten aufbewahrt werden sollten, obwohl sie für den eigentlichen Verarbeitungszweck nicht mehr bebraucht werden (zB Austellung eines Dienstzeugnisses bis zu 30 Jahre nach Beendigung des Dienstverhältnisses).
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	erledigt und dokumentiert

Maßnahme:	**M_DSMS_008 Zwecke für Verarbeitungstätigkeiten definieren und Legitimität überprüfen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Definieren Sie vor Beginn jeder Verarbeitungstätigkeit den konkreten Zweck und überprüfen Sie, ob dieser im Einklang mit gesetzlichen Anforderungen steht (zB aus dem Arbeits- oder Vertragsrecht). Die Definition des Zwecks ist nicht nur zur Erfüllung der Informationspflicht gegenüber den Betroffenen relevant, sondern hat auch Auswirkungen auf die Speicherdauer und die erforderlichen Daten und somit Einfluss auf die Grundsätze "Speicherbegrenzung" und "Datenminimierung".
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	Zwecke für alle derzeit dokumentierten VTs definiert und überprüft

Art. 05 Abs. 1 lit. c "Datenminimierung"

Art. 05 Abs. 1 lit. d "Richtigkeit"

Art. 05 Abs. 1 lit. e "Speicherbegrenzung"

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_006 gesetzliche Aufbewahrungspflichten überprüfen**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Überprüfen Sie für jede Verarbeitungstätigkeit, ob es für die personenbezogenen Daten gesetzliche Aufbewahrungspflichten gibt, die einer frühzeitigen Löschung dieser Daten entegegenstehen. Überprüfen Sie des Weiteren, ob es gesetzliche Verpflichtungen gibt, für die gewisse personenbezogene Daten aufbewahrt werden sollten, obwohl sie für den eigentlichen Verarbeitungszweck nicht mehr bebraucht werden (zB Austellung eines Dienstzeugnisses bis zu 30 Jahre nach Beendigung des Dienstverhältnisses).
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	erledigt und dokumentiert

Art. 05 Abs. 1 lit. f "Integrität und Vertraulichkeit"

Offene Maßnahmen:

Maßnahme:	**M_DSMS_034 Vertraulichkeit, Verfügbarkeit und Integrität personenbezogener Daten sicherstellen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Setzen Sie Maßnahmen um, die die Vertraulichkeit, Verfügbarkeit und Integrität personenbezogener Daten sicherstellen. Sehen Sie dazu genauere Anweisungen im Kapitel "Technische und Organisatorische Maßnahmen" in dieser Wissensdatenbank zur DSGVO und beachten Sie auch Vorgaben aus dem Informationssicherheitsmanagement (zB auch die Wisssensdatenbank zur Umsetzung der ISO 27001). Mit den bereits gesetzten Maßnahmen im ISMS abgleichen.
Fortschritt:	0%

Art. 05 Abs. 2 "Rechenschaftspflicht"

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_024 Erfüllung der Rechenschaftspflicht sicherstellen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Setzen Sie Maßnahmen, um die Einhaltung der Datenschutzgrundsätze nachweisen zu können. Dokumentieren Sie dazu alle relevanten Maßnahmen und Prozesse, wie zB: - Datenschutzrichtlinie/ Datenschutzkonzept/Datenschutzmanagement - Benennung eines Datenschutzbeauftragten und Regelung aller datenschutzrelevanten Verantwortlichkeiten - Führen des Verzeichnisses von Verarbeitungstätigkeiten - transparente Prozesse zur Erfüllung der Betroffenenrechte - effektive Prozesse zur Behandlung von Datenschutzverletzungen - Überwachung der Umsetzung und Tauglichkeit gesetzter Maßnahmen
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	Prozedere definiert

Art. 06 Rechtmäßigkeit der Verabeitung

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_009 Rechtsgrundlage für Verarbeitungstätigkeiten überprüfen und dokumentieren**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Überprüfen Sie für jede von Ihnen durchgeführte Verarbeitungstätigkeit, ob eine gültige Rechtsgrundlage besteht. Die gängigsten Bedingungen für eine rechtmäßige Verarbeitung sind : - die Einwilligung der betroffenen Person - die Vertragserfüllung bzw. die Durchführung vorvertraglicher Maßnahmen - die Erfüllung einer rechtlichen Verpflichtung Dokumentieren Sie die Rechtsgrundlage für jede Verarbeitungstätigkeit (zB direkt im Verzeichnis von Verarbeitungstätigkeiten).
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	erledigt- siehe VVT

Art. 06 Abs. 01 Rechtmäßigkeit

Art. 06 Abs. 1 lit. a Einwilligung

Art. 06 Abs. 1 lit. b Vertragserfüllung / vorvertragliche Verpflichtungen

Art. 06 Abs. 1 lit. c gesetzliche Verpflichtungen

Art. 06 Abs. 1 lit. d lebenswichtige Interessen

Art. 06 Abs. 1 lit. e öffentliche Interessen

Art. 06 Abs. 1 lit. f berechtigte Interessen des Verantwortlichen / eines Dritten

Art. 06 Abs. 02 Anpassung durch die Mitgliedsstaaten

Art. 06 Abs. 03 Festlegung der Rechtsgrundlage

Art. 06 Abs. 04 Zweckänderung

Art. 07 Bedingungen für die Einwilligung

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_020 Hinweis auf Widerrufsrecht in Datenschutzerklärungen einbinden**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Beziehen sich Datenschutzerklärungen auf Datenverarbeitungen, die auf einer Einwilligung beruhen, so ist der Hinweis auf das Widerrufsrecht auch in der Datenschutzerklärung aufzunehmen.
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	bestehende DS-Erklärungen auf aktuellem Stand

Art. 08 Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft

Keine zugewiesenen Maßnahmen

Art. 09 Verarbeitung beonderer Kategorien personenbezogener Daten

Keine zugewiesenen Maßnahmen

Art. 09 Abs. 1 Definition

Keine zugewiesenen Maßnahmen

Art. 09 Abs. 2 Erlaubnistatbestand

Keine zugewiesenen Maßnahmen

Art. 09 Abs. 2 lit. a Einwilligung

Keine zugewiesenen Maßnahmen

Art. 09 Abs. 2 lit. b Arbeitsrecht und soziale Sicherheit

Keine zugewiesenen Maßnahmen

Art. 09 Abs. 2 lit. c lebenswichtige Interessen

Keine zugewiesenen Maßnahmen

Art. 09 Abs. 2 lit. d Mitgliederverwaltung von Kirchen, Gewerkschaften, etc.

Keine zugewiesenen Maßnahmen

Art. 09 Abs. 2 lit. e selbst öffentlich gemacht

Keine zugewiesenen Maßnahmen

Art. 09 Abs. 2 lit. f Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

Keine zugewiesenen Maßnahmen

Art. 09 Abs. 2 lit. g erhebliches öffentliches Interesse

Keine zugewiesenen Maßnahmen

Art. 09 Abs. 2 lit. h Gesundheitsvorsorge

Keine zugewiesenen Maßnahmen

Art. 09 Abs. 2 lit. i öffentliche Gesundheit

Keine zugewiesenen Maßnahmen

Art. 09 Abs. 2 lit. j Archivzwecke, wissenschaftliche und historische Forschung

Keine zugewiesenen Maßnahmen

Art. 09 Abs. 3 Standesrecht für Gesundheitsberufe / Berufsgeheimnis

Keine zugewiesenen Maßnahmen

Art. 09 Abs. 4 weitere Einschränkungen

Keine zugewiesenen Maßnahmen

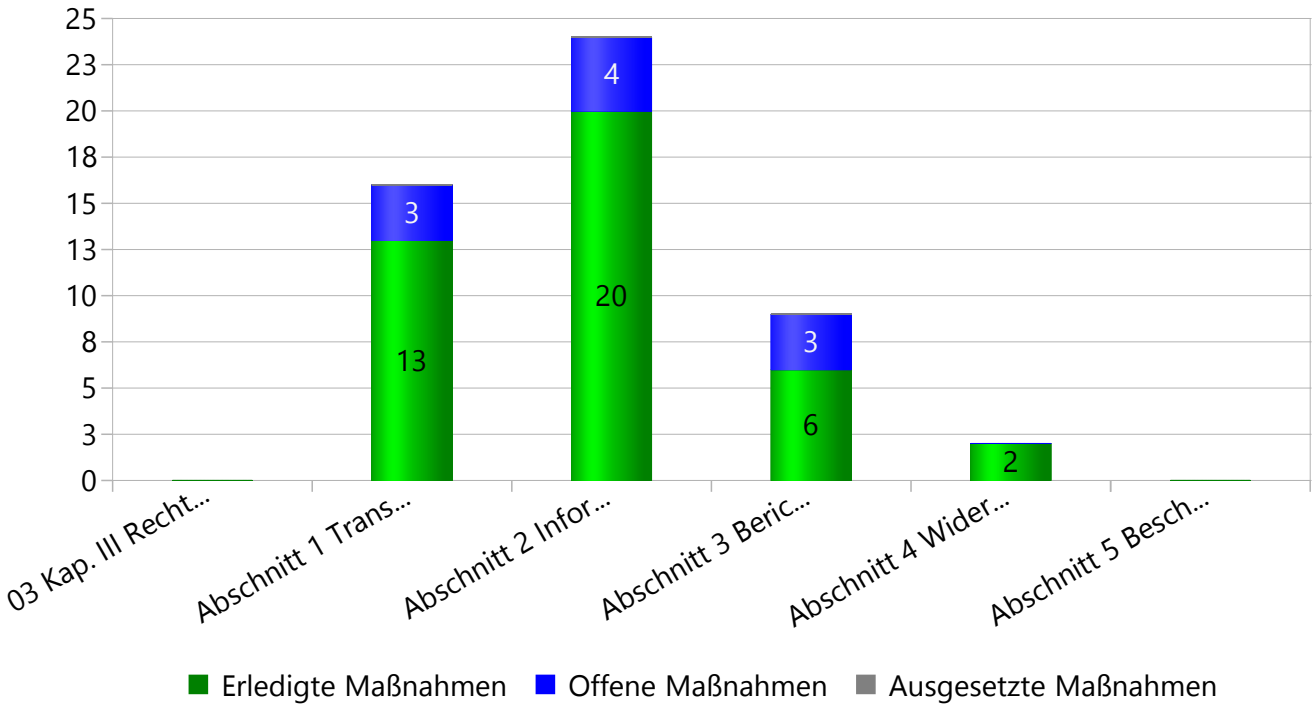
Art. 10 Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten

Keine zugewiesenen Maßnahmen

Art. 11 Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist

Keine zugewiesenen Maßnahmen

03 Kap. III Rechte der betroffenen Person



Abschnitt 1 Transparenz und Modalitäten

Offene Maßnahmen:

Maßnahme:	**M_DSMS_036 Nutzung diverser Social-Media-Kanäle überdenken**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	einige Social-Media-Kanäle sind datenschutzrechtliche bedenklich. Kanäle, die nicht primär genutzt werden, sollten aussortiert werden und für die restlichen, die von hoher Relevanz sind, muss ggf. ein geeignetes Verfahren zur Wahrung des Datenschutzes erarbeitet werden. Dabei sind insbesondere die Informationspflichten zu beachten.
Fortschritt:	0%
Maßnahme:	**M_DSMS_038 Datenschutzerklärung bzgl. Remarketing-Aktivitäten ergänzen**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Der Einsatz von Remarketing-Tools auf der Website wird derzeit überarbeitet. Diesbzgl. muss überprüft werden, inwieweit die Datenschutzerklärung auf der Homepage angepasst werden muss.
Fortschritt:	0%

Art. 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

Offene Maßnahmen:

Maßnahme:	**M_DSMS_033 Zugang zur Datenschutzerklärung für Bewerber schaffen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Bewerber sollten im Zuge ihrer Bewerbung eine Datenschutzerklärung zur Verarbeitung ihrer personenbezogenen Daten erhalten. Es empfiehlt sich eine solche auf der Homepage einzubinden. Wenn die Möglichkeit einer Online-Bewerbung besteht bzw. Stellen online ausgeschrieben werden, sollte auf die relevante Datenschutzerklärung verlinkt werden.
Fortschritt:	0%

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_010 DSGVO-konforme Datenschutzerklärung erstellen**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Stellen Sie sicher, dass Ihre Datenschutzerklärungen alle geforderten Informationen enthalten. Dazu gehören grundsätzlich: - Namen und Kontaktdaten des Verantwortlichen (ggf. seines Vertreters) - Kontaktdaten des Datenschutzbeauftragten, wenn im Unternehmen einer bestellt ist - die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen - die Rechtsgrundlage für die Verarbeitung (insbesondere ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben ist oder für einen Vertragsabschluss erforderlich ist und ob die betroffene Person zur Bereitstellung der Daten verpflichtet ist und welche Folgen eine Nichtbereitstellung hätte Art 13 Abs 2 lit e) - die berechtigten Interessen des Verantwortlichen bzw. eines Dritten, wenn die Verarbeitung auf solchen beruht - die Empfänger oder Empfängerkategorien der personenbezogenen Daten, wenn personenbezogene Daten solchen offengelegt werden - die Übermittlung der personenbezogenen Daten an ein Drittland oder eine internationale Organisation, wenn eine solche geplant ist, sowie die Rechtsgrundlage einer solchen Übermittlung - die Speicherdauer der personenbezogenen Daten oder, wenn keine genaue Frist angegeben werden kann, zumindest die Kriterien für die Festlegung der Dauer - ein Hinweis auf die Möglichkeit der Ausübung der Rechte auf Auskunft, Löschung, Berichtigung, Widerspruch, Einschränkung und Datenübertragbarkeit - ein Hinweis darauf, dass erteilte Einwilligungen jederzeit widerrufen werden können, jedoch die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung davon nicht berührt wird - ein Hinweis auf das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde - aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und Auswirkungen für den Betroffen, wenn eine automatisierte Entscheidungsfindung besteht - maßgebliche Informationen im Zuge einer Zweckänderung bei der Weiterverarbeitung der personenbezogenen Daten Beachten Sie, dass Sie Betroffene auch über die Herkunft der Daten informieren müssen, falls diese nicht direkt bei der betroffenen Person erhoben wurden. Diese Informationen sind dann nicht zu erteilen, wenn die betroffene Person bereits über die Informationen verfügt.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	erledigt

Maßnahme:	**M_DSMS_011 Datenschutzerklärung auf Homepage einbinden**
OrgEH:	IT Abteilung TeSA (TeSA_IT)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Die Datenschutzerklärung muss auf der Homepage leicht auffindbar sein. Dazu muss die Datenschutzerklärung über einen eigenen Link von jeder Seite aus erreichbar sein. Stellen Sie im Zuge dessen auch sicher, dass alle Verarbeitungen, die im Zuge der Bereitstellung Ihrer Homepage getätigt werden, in der Datenschutzerklärung angeführt sind. Denken Sie dabei insbesondere an - den Einsatz von Cookies, Analyse- und Remarketingtools (zB Google Analytics, Google Adwords, etc - Daten, die Sie im Zuge von Kontaktformularen, Newslettern oder Blogs verarbeiten - die Verwendung von Social-Media Plugins - etwaige Chatfunktionen -...
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	erledigt

Maßnahme:	**M_DSMS_012 Online-Formular für Datenschutzanfragen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Betroffenen kann ein Online-Formular zur Verfügung gestellt werden, über welches Anfragen iZm personenbezogenen Daten gestellt werden können. Es empfiehlt sich, den Betroffenen darauf hinzuweisen, dass unter gegebenen Umständen ein Identitätsnachweis erforderlich ist.
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	seit Juni online

Maßnahme:	**M_DSMS_013 Zentrale Anlaufstelle für Betroffenenrechte schaffen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Für Betroffene muss die Ausübung ihrer Rechte einfach gestaltet werden. Dazu gehört die Möglichkeit, rasch den richtigen Ansprechpartner für Datenschutzfragen ermitteln zu können. Es empfiehlt sich daher eine eigene Email-Adresse für Datenschutzangelegenheiten einzurichten und/oder ein Online-Formular für Betroffenenanfragen zur Verfügung zu stellen. Es ist jedenfalls sicherzustellen, dass die Anfragen über diese Emai-Adresse bzw. das Online-Formular rasch bearbeitet werden, um die Fristen zur Beantwortung von Betroffenenanfragen einhalten zu können.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	Email-Adresse eingerichtet

Maßnahme:	**M_DSMS_014 Prozess zur Identitätsprüfung einführen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Die Betroffenenrechte stehen grundsätzlich nur der betroffenen Person selbst zu. Es sollten daher alle vertretbaren Mittel genutzt werden, um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen. Wenn begründete Zweifel an der Identität bestehen und ein Identitätsnachweis nicht erbracht werden kann, darf die Anfrage nicht erfüllt werden. Um Anfragen von Betroffenen rechtmäßig bearbeiten zu können, muss daher die Identität der betroffenen Person festgestellt werden. Dazu sollte ein Prozess etabliert werden, der sicherstellt, dass allen, die Betroffenenanfragen bearbeiten, klar ist, - unter welchen Umständen ein Identitätsnachweis anzufordern ist - welche Art des Identitätsnachweis in der jeweiligen Situation erforderlich ist - wie mit dem Identitätsnachweis nach Feststellung der Identität zu verfahren ist Wenn Zweifel an der Identität der natürlichen Person, die ein Betroffenenrecht geltend macht, bestehen, so kann der Verantwortliche von der Person zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind. Insbesondere bei telefonischen Anfragen oder Anfragen über eine Fantasieemailadresse können Zweifel an der Identität des Antragstellers bestehen.
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	erledigt

Maßnahme:	**M_DSMS_015 Bearbeitung von Betroffenenanfragen dokumentieren**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Dokumentieren Sie für jede Betroffenenanfrage insbesondere folgende Punkte: - Zeitablauf: Eingang der Anfrage, Beantwortung der Anfrage - Identitätsverifizierung bzw. Identifizierungsmaßnahmen - gegebenenfalls Verweigerungsgründe - gesetzte Maßnahmen iZm der Anfrage - Art der Kommunikation Eine ordnungsgemäße Dokumentation kann auch helfen, den Nachweis für exzessive Anfragen zu unterstützen.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	Prozess definiert und kommuniziert

Maßnahme:	**M_DSMS_016 Erstellen eines Daten-Mapping-Systems**
OrgEH:	IT Abteilung TeSA (TeSA_IT)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Um die Anforderungen in Bezug auf die Betroffenenrechte gesetzeskonform erfüllen zu können, sollte der Lebenszyklus personenbezogener Daten im Unternehmen festgestellt werden. Es soll feststellbar sein, wo personenbezogene Daten zugänglich sind (Syteme, Applilkationen, etc.), damit schnell identifiziert werden kann, ob personenbezogene Daten vorhanden sind und wo überall sie vorhanden sind und unter welchen Bedingungen sie vorhanden sind. Weiters soll ersichtlich sein, an wen die Daten übermittelt werden, um die Empfänger der Daten leicht ermitteln zu können. Folgendes ist zu dokumentieren: Datenflüsse, Datentransfers zwischen Systemen und Kategorisierung von Systemen nach den Datentransfers. Über eine Datenlandkarte (Daten-Mapping) sollen alle zu einer Person vorliegenden Daten applikationsübergreifend vollständig und lückenlos dargestellt werden. Jedes Datenobjekt kann so mit den Verarbeitungstätigkeiten und rechtlichen Grundlagen sowie den Verarbeitungszwecken verknüpft werden. Im Zuge eines Löschungsbegehrens kann so sichergestellt werden, dass die Daten auf allen Systemen gelöscht werden.
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	fertiggestellt

Maßnahme:	**M_DSMS_017 Musterschreiben Recht auf Auskunft**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Um ein Auskunftsbegehren vollständig und fristgerecht zu beantworten, sollten Musterschreiben vorbereitet werden, die nur mehr an die spezielle Betroffenenanfrage angepasst werden müssen. Ein solches Musterschreiben kann vorgefertigte Textbausteine enthalten, die grundsätzlich folgende Szenarien und Inhalte abdecken sollten: - Hinweis, wenn begründete Zweifel an der Identität der betroffenen Person bestehen (mit Aufforderung zum Identitätsnachweis) - Hinweis auf Fristverlängerung (inkl. Begründung) - Negativauskunft (wenn keine personenbezogenen Daten verarbeitet werden) - Positivauskunft (wenn personenebezogene Daten verarbeitet werden) mit einer Aufstellung der verarbeiteten personenbezogenen Daten, sowie der zusätzlichen in Art 15 Abs 1 geforderten Informationen -> Zwecke und Rechtsgrundlagen der Verarbeitung, Empfänger (insb. Empfänger in Drittländern), Speicherdauer, Herkunft der Daten (wenn sie nicht von der betroffenen Person stammen), Bestehen einer automatisierten Entscheidungsfindung (einschließlich Profiling) inkl. Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen, geeignete Garantien iZm Übermittlung in Drittländer - Information über das Bestehen eines Rechts auf Berichtigung, Löschung, Einschränkung, Widerspruch - Information über Beschwerderecht bei einer Aufsichtsbehörde - Begründung für etwaige Auskunftsverweigerung (inkl. Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde bzw. auf Möglichkeit eines gerichtlichen Rechtsbehelfs) - Begründung für etwaige Kostenersatzforderung (gem. Art 15 Abs 3 oder Art 12 Abs 5 lit a)
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	erstellt

Maßnahme:	**M_DSMS_020 Hinweis auf Widerrufsrecht in Datenschutzerklärungen einbinden**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Beziehen sich Datenschutzerklärungen auf Datenverarbeitungen, die auf einer Einwilligung beruhen, so ist der Hinweis auf das Widerrufsrecht auch in der Datenschutzerklärung aufzunehmen.
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	bestehende DS-Erklärungen auf aktuellem Stand

Maßnahme:	**M_DSMS_022 Datenschutzerklärung in Social-Media-Kanäle einbinden**
OrgEH:	IT Abteilung TeSA (TeSA_IT)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Wenn sich das Unternehmen auf Social-Media-Kanälen repräsentiert, sollte auch dort eine entsprechende Datenschutzerklärung vorgehalten werden. Dies betrifft insbesondere Facebook (siehe EuGH-Urteil ECLI "EU:C:2018:388"), kann aber auch auf andere Werbekanäle wie Instagram, Twitter, etc. umgemünzt werden. Die Auswirkungen dieses Urteils auf die Praxis sind noch offen. Es empfiehlt sich aber jedenfalls eine Datenschutzerklärung auf diesen Werbekanälen zu integrieren. Es kann dabei beispielsweise so vorgegangen werden: Bei Facebook kann zB unter "Info" ein Link zur Datenschutzerklärung untergebracht werden. Dabei sollte in der Datenschutzerklärung auf die Zwecke und den Umfang der Facebook-Nutzung durch das Unternehmen hingewiesen werden. Für die Nutzung der Daten durch Facebook kann auf die Datenrichtlinie von Facebook verwiesen werden.
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	Datenschutzerklärung ist in allen Kanälen integriert

Maßnahme:	**M_DSMS_023 Zugang zur Datenschutzerklärung für Mitarbeiter schaffen**
OrgEH:	Personalabteilung TeSA (TeSA_PER)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Mitarbeiter sollten im Zuge der Einstellung und der regelmäßigen Datenschutz-Schulung über die Verarbeitung sie betreffender personenbezogener Daten informiert werden und in weiterer Folge Zugriff zur für sie relevanten Datenschutzerklärung haben. Dies kann zB durch Aushändigen einer Kopie oder Verweis auf ein Dokument in einem jederzeit zugänglichen Ordner (online/offline) oder durch Zugriff über ein Intranet erfolgen.
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	an alle kommunziert und am Z-Laufwerk jederzeit abrufbar

Maßnahme:	**M_DSMS_031 Musterschreiben Recht auf Widerspruch**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Um einen Widerspruch vollständig und fristgerecht zu beantworten, sollten Musterschreiben vorbereitet werden, die nur mehr an die spezielle Betroffenenanfrage angepasst werden müssen. Ein solches Musterschreiben kann vorgefertigte Textbausteine enthalten, die folgende Szenarien und Inhalte abdecken sollten: - Hinweis, wenn begründete Zweifel an der Identität der betroffenen Person bestehen mit Aufforderung zum Identitätsnachweis) - Hinweis auf etwaige Fristverlängerung (inkl. Begründung) - Negativauskunft, falls keine personenbezogenen Daten des Betroffenen verarbeitet werden - Information darüber, dass keine Maßnahmen in Bezug auf den Widerspruch vorgenommen wurden (inkl. der Gründe dafür und dem Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde bzw. auf Möglichkeit eines gerichtlichen Rechtsbehelfs) - bzw. Information darüber, dass Maßnahmen in Bezug auf den Widerspruch vorgenommen wurden - Begründung für etwaige Kostenersatzforderung (gem. Art 12 Abs 5 lit a)
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	ist erledigt - siehe Anhang

Maßnahme:	**M_DSMS_032 Hinweis auf Beschwerderecht in Datenschutzerklärungen**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Sämtliche Datenschutzerklärungen sind dahingehend zu überprüfen, ob der Hinweis auf das Beschwerderecht bei einer Aufsichtsbehörde enthalten ist. Jede betroffene Person hat das Recht, sich bei einer Aufsichtsbehörde zu beschweren, wenn sie der Ansicht ist, dass eine Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt (Art 77).
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	ist aufgenommen - aktualisierte Erklärung im Anhang

Abschnitt 2 Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten

Offene Maßnahmen:

Maßnahme:	**M_DSMS_036 Nutzung diverser Social-Media-Kanäle überdenken**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	einige Social-Media-Kanäle sind datenschutzrechtliche bedenklich. Kanäle, die nicht primär genutzt werden, sollten aussortiert werden und für die restlichen, die von hoher Relevanz sind, muss ggf. ein geeignetes Verfahren zur Wahrung des Datenschutzes erarbeitet werden. Dabei sind insbesondere die Informationspflichten zu beachten.
Fortschritt:	0%

Art. 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

Offene Maßnahmen:

Maßnahme:	**M_DSMS_037 Datenschutzerklärungen für alle relevanten Interessensgruppen erstellen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Erstellen Sie für alle Interessensgruppen Datenschutzerklärungen, um der Informationspflicht nachzukommen. Stellen Sie sicher, dass für alle Betroffenenkategorien, über die Sie personenbezogene Daten verarbeiten, Datenschutzerklärungen vorhanden sind, die über alle für die jeweiligen Beroffenen relevanten durchgeführten Verarbeitungen ausreichend informieren (siehe M_INF_001a zur Erstellung einer DSGVO-konformen Datenschutzerklärung). Stellen Sie darüberhinaus sicher, dass diese Erklärungen auch rechtzeitig kommuniziert werden. Denken Sie dabei insbesondere an - Mitarbeiter - Bewerber - Interessenten - Kunden - Lieferanten - Geschäftspartner - Websitebesucher - etc.
Fortschritt:	0%
Maßnahme:	**M_DSMS_033 Zugang zur Datenschutzerklärung für Bewerber schaffen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Bewerber sollten im Zuge ihrer Bewerbung eine Datenschutzerklärung zur Verarbeitung ihrer personenbezogenen Daten erhalten. Es empfiehlt sich eine solche auf der Homepage einzubinden. Wenn die Möglichkeit einer Online-Bewerbung besteht bzw. Stellen online ausgeschrieben werden, sollte auf die relevante Datenschutzerklärung verlinkt werden.
Fortschritt:	0%

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_010 DSGVO-konforme Datenschutzerklärung erstellen**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Stellen Sie sicher, dass Ihre Datenschutzerklärungen alle geforderten Informationen enthalten. Dazu gehören grundsätzlich: - Namen und Kontaktdaten des Verantwortlichen (ggf. seines Vertreters) - Kontaktdaten des Datenschutzbeauftragten, wenn im Unternehmen einer bestellt ist - die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen - die Rechtsgrundlage für die Verarbeitung (insbesondere ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben ist oder für einen Vertragsabschluss erforderlich ist und ob die betroffene Person zur Bereitstellung der Daten verpflichtet ist und welche Folgen eine Nichtbereitstellung hätte Art 13 Abs 2 lit e) - die berechtigten Interessen des Verantwortlichen bzw. eines Dritten, wenn die Verarbeitung auf solchen beruht - die Empfänger oder Empfängerkategorien der personenbezogenen Daten, wenn personenbezogene Daten solchen offengelegt werden - die Übermittlung der personenbezogenen Daten an ein Drittland oder eine internationale Organisation, wenn eine solche geplant ist, sowie die Rechtsgrundlage einer solchen Übermittlung - die Speicherdauer der personenbezogenen Daten oder, wenn keine genaue Frist angegeben werden kann, zumindest die Kriterien für die Festlegung der Dauer - ein Hinweis auf die Möglichkeit der Ausübung der Rechte auf Auskunft, Löschung, Berichtigung, Widerspruch, Einschränkung und Datenübertragbarkeit - ein Hinweis darauf, dass erteilte Einwilligungen jederzeit widerrufen werden können, jedoch die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung davon nicht berührt wird - ein Hinweis auf das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde - aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und Auswirkungen für den Betroffen, wenn eine automatisierte Entscheidungsfindung besteht - maßgebliche Informationen im Zuge einer Zweckänderung bei der Weiterverarbeitung der personenbezogenen Daten Beachten Sie, dass Sie Betroffene auch über die Herkunft der Daten informieren müssen, falls diese nicht direkt bei der betroffenen Person erhoben wurden. Diese Informationen sind dann nicht zu erteilen, wenn die betroffene Person bereits über die Informationen verfügt.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	erledigt

Maßnahme:	**M_DSMS_011 Datenschutzerklärung auf Homepage einbinden**
OrgEH:	IT Abteilung TeSA (TeSA_IT)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Die Datenschutzerklärung muss auf der Homepage leicht auffindbar sein. Dazu muss die Datenschutzerklärung über einen eigenen Link von jeder Seite aus erreichbar sein. Stellen Sie im Zuge dessen auch sicher, dass alle Verarbeitungen, die im Zuge der Bereitstellung Ihrer Homepage getätigt werden, in der Datenschutzerklärung angeführt sind. Denken Sie dabei insbesondere an - den Einsatz von Cookies, Analyse- und Remarketingtools (zB Google Analytics, Google Adwords, etc - Daten, die Sie im Zuge von Kontaktformularen, Newslettern oder Blogs verarbeiten - die Verwendung von Social-Media Plugins - etwaige Chatfunktionen -...
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	erledigt

Maßnahme:	**M_DSMS_016 Erstellen eines Daten-Mapping-Systems**
OrgEH:	IT Abteilung TeSA (TeSA_IT)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Um die Anforderungen in Bezug auf die Betroffenenrechte gesetzeskonform erfüllen zu können, sollte der Lebenszyklus personenbezogener Daten im Unternehmen festgestellt werden. Es soll feststellbar sein, wo personenbezogene Daten zugänglich sind (Syteme, Applilkationen, etc.), damit schnell identifiziert werden kann, ob personenbezogene Daten vorhanden sind und wo überall sie vorhanden sind und unter welchen Bedingungen sie vorhanden sind. Weiters soll ersichtlich sein, an wen die Daten übermittelt werden, um die Empfänger der Daten leicht ermitteln zu können. Folgendes ist zu dokumentieren: Datenflüsse, Datentransfers zwischen Systemen und Kategorisierung von Systemen nach den Datentransfers. Über eine Datenlandkarte (Daten-Mapping) sollen alle zu einer Person vorliegenden Daten applikationsübergreifend vollständig und lückenlos dargestellt werden. Jedes Datenobjekt kann so mit den Verarbeitungstätigkeiten und rechtlichen Grundlagen sowie den Verarbeitungszwecken verknüpft werden. Im Zuge eines Löschungsbegehrens kann so sichergestellt werden, dass die Daten auf allen Systemen gelöscht werden.
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	fertiggestellt

Maßnahme:	**M_DSMS_020 Hinweis auf Widerrufsrecht in Datenschutzerklärungen einbinden**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Beziehen sich Datenschutzerklärungen auf Datenverarbeitungen, die auf einer Einwilligung beruhen, so ist der Hinweis auf das Widerrufsrecht auch in der Datenschutzerklärung aufzunehmen.
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	bestehende DS-Erklärungen auf aktuellem Stand

Maßnahme:	**M_DSMS_022 Datenschutzerklärung in Social-Media-Kanäle einbinden**
OrgEH:	IT Abteilung TeSA (TeSA_IT)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Wenn sich das Unternehmen auf Social-Media-Kanälen repräsentiert, sollte auch dort eine entsprechende Datenschutzerklärung vorgehalten werden. Dies betrifft insbesondere Facebook (siehe EuGH-Urteil ECLI "EU:C:2018:388"), kann aber auch auf andere Werbekanäle wie Instagram, Twitter, etc. umgemünzt werden. Die Auswirkungen dieses Urteils auf die Praxis sind noch offen. Es empfiehlt sich aber jedenfalls eine Datenschutzerklärung auf diesen Werbekanälen zu integrieren. Es kann dabei beispielsweise so vorgegangen werden: Bei Facebook kann zB unter "Info" ein Link zur Datenschutzerklärung untergebracht werden. Dabei sollte in der Datenschutzerklärung auf die Zwecke und den Umfang der Facebook-Nutzung durch das Unternehmen hingewiesen werden. Für die Nutzung der Daten durch Facebook kann auf die Datenrichtlinie von Facebook verwiesen werden.
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	Datenschutzerklärung ist in allen Kanälen integriert

Maßnahme:	**M_DSMS_023 Zugang zur Datenschutzerklärung für Mitarbeiter schaffen**
OrgEH:	Personalabteilung TeSA (TeSA_PER)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Mitarbeiter sollten im Zuge der Einstellung und der regelmäßigen Datenschutz-Schulung über die Verarbeitung sie betreffender personenbezogener Daten informiert werden und in weiterer Folge Zugriff zur für sie relevanten Datenschutzerklärung haben. Dies kann zB durch Aushändigen einer Kopie oder Verweis auf ein Dokument in einem jederzeit zugänglichen Ordner (online/offline) oder durch Zugriff über ein Intranet erfolgen.
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	an alle kommunziert und am Z-Laufwerk jederzeit abrufbar

Maßnahme:	**M_DSMS_032 Hinweis auf Beschwerderecht in Datenschutzerklärungen**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Sämtliche Datenschutzerklärungen sind dahingehend zu überprüfen, ob der Hinweis auf das Beschwerderecht bei einer Aufsichtsbehörde enthalten ist. Jede betroffene Person hat das Recht, sich bei einer Aufsichtsbehörde zu beschweren, wenn sie der Ansicht ist, dass eine Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt (Art 77).
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	ist aufgenommen - aktualisierte Erklärung im Anhang

Maßnahme:	**M_DSMS_039 Datenschutzerklärung für Mitarbeiter und Datenschutzrichtlinie in Onboarding-Prozess einbinden**
OrgEH:	Personalabteilung TeSA (TeSA_PER)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Die Datenschutzerklärung für Mitarbeiter und die Datenschutzrichtlinie muss in die Willkommensmappe für neue Mitarbeiter integriert werden und fixer Bestandteil des Onboarding-Prozesses sein
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	ist in Willkommensmappe integriert.

Art. 14 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

Offene Maßnahmen:

Maßnahme:	**M_DSMS_037 Datenschutzerklärungen für alle relevanten Interessensgruppen erstellen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Erstellen Sie für alle Interessensgruppen Datenschutzerklärungen, um der Informationspflicht nachzukommen. Stellen Sie sicher, dass für alle Betroffenenkategorien, über die Sie personenbezogene Daten verarbeiten, Datenschutzerklärungen vorhanden sind, die über alle für die jeweiligen Beroffenen relevanten durchgeführten Verarbeitungen ausreichend informieren (siehe M_INF_001a zur Erstellung einer DSGVO-konformen Datenschutzerklärung). Stellen Sie darüberhinaus sicher, dass diese Erklärungen auch rechtzeitig kommuniziert werden. Denken Sie dabei insbesondere an - Mitarbeiter - Bewerber - Interessenten - Kunden - Lieferanten - Geschäftspartner - Websitebesucher - etc.
Fortschritt:	0%

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_010 DSGVO-konforme Datenschutzerklärung erstellen**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Stellen Sie sicher, dass Ihre Datenschutzerklärungen alle geforderten Informationen enthalten. Dazu gehören grundsätzlich: - Namen und Kontaktdaten des Verantwortlichen (ggf. seines Vertreters) - Kontaktdaten des Datenschutzbeauftragten, wenn im Unternehmen einer bestellt ist - die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen - die Rechtsgrundlage für die Verarbeitung (insbesondere ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben ist oder für einen Vertragsabschluss erforderlich ist und ob die betroffene Person zur Bereitstellung der Daten verpflichtet ist und welche Folgen eine Nichtbereitstellung hätte Art 13 Abs 2 lit e) - die berechtigten Interessen des Verantwortlichen bzw. eines Dritten, wenn die Verarbeitung auf solchen beruht - die Empfänger oder Empfängerkategorien der personenbezogenen Daten, wenn personenbezogene Daten solchen offengelegt werden - die Übermittlung der personenbezogenen Daten an ein Drittland oder eine internationale Organisation, wenn eine solche geplant ist, sowie die Rechtsgrundlage einer solchen Übermittlung - die Speicherdauer der personenbezogenen Daten oder, wenn keine genaue Frist angegeben werden kann, zumindest die Kriterien für die Festlegung der Dauer - ein Hinweis auf die Möglichkeit der Ausübung der Rechte auf Auskunft, Löschung, Berichtigung, Widerspruch, Einschränkung und Datenübertragbarkeit - ein Hinweis darauf, dass erteilte Einwilligungen jederzeit widerrufen werden können, jedoch die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung davon nicht berührt wird - ein Hinweis auf das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde - aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und Auswirkungen für den Betroffen, wenn eine automatisierte Entscheidungsfindung besteht - maßgebliche Informationen im Zuge einer Zweckänderung bei der Weiterverarbeitung der personenbezogenen Daten Beachten Sie, dass Sie Betroffene auch über die Herkunft der Daten informieren müssen, falls diese nicht direkt bei der betroffenen Person erhoben wurden. Diese Informationen sind dann nicht zu erteilen, wenn die betroffene Person bereits über die Informationen verfügt.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	erledigt

Maßnahme:	**M_DSMS_011 Datenschutzerklärung auf Homepage einbinden**
OrgEH:	IT Abteilung TeSA (TeSA_IT)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Die Datenschutzerklärung muss auf der Homepage leicht auffindbar sein. Dazu muss die Datenschutzerklärung über einen eigenen Link von jeder Seite aus erreichbar sein. Stellen Sie im Zuge dessen auch sicher, dass alle Verarbeitungen, die im Zuge der Bereitstellung Ihrer Homepage getätigt werden, in der Datenschutzerklärung angeführt sind. Denken Sie dabei insbesondere an - den Einsatz von Cookies, Analyse- und Remarketingtools (zB Google Analytics, Google Adwords, etc - Daten, die Sie im Zuge von Kontaktformularen, Newslettern oder Blogs verarbeiten - die Verwendung von Social-Media Plugins - etwaige Chatfunktionen -...
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	erledigt

Maßnahme:	**M_DSMS_016 Erstellen eines Daten-Mapping-Systems**
OrgEH:	IT Abteilung TeSA (TeSA_IT)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Um die Anforderungen in Bezug auf die Betroffenenrechte gesetzeskonform erfüllen zu können, sollte der Lebenszyklus personenbezogener Daten im Unternehmen festgestellt werden. Es soll feststellbar sein, wo personenbezogene Daten zugänglich sind (Syteme, Applilkationen, etc.), damit schnell identifiziert werden kann, ob personenbezogene Daten vorhanden sind und wo überall sie vorhanden sind und unter welchen Bedingungen sie vorhanden sind. Weiters soll ersichtlich sein, an wen die Daten übermittelt werden, um die Empfänger der Daten leicht ermitteln zu können. Folgendes ist zu dokumentieren: Datenflüsse, Datentransfers zwischen Systemen und Kategorisierung von Systemen nach den Datentransfers. Über eine Datenlandkarte (Daten-Mapping) sollen alle zu einer Person vorliegenden Daten applikationsübergreifend vollständig und lückenlos dargestellt werden. Jedes Datenobjekt kann so mit den Verarbeitungstätigkeiten und rechtlichen Grundlagen sowie den Verarbeitungszwecken verknüpft werden. Im Zuge eines Löschungsbegehrens kann so sichergestellt werden, dass die Daten auf allen Systemen gelöscht werden.
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	fertiggestellt

Maßnahme:	**M_DSMS_020 Hinweis auf Widerrufsrecht in Datenschutzerklärungen einbinden**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Beziehen sich Datenschutzerklärungen auf Datenverarbeitungen, die auf einer Einwilligung beruhen, so ist der Hinweis auf das Widerrufsrecht auch in der Datenschutzerklärung aufzunehmen.
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	bestehende DS-Erklärungen auf aktuellem Stand

Maßnahme:	**M_DSMS_022 Datenschutzerklärung in Social-Media-Kanäle einbinden**
OrgEH:	IT Abteilung TeSA (TeSA_IT)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Wenn sich das Unternehmen auf Social-Media-Kanälen repräsentiert, sollte auch dort eine entsprechende Datenschutzerklärung vorgehalten werden. Dies betrifft insbesondere Facebook (siehe EuGH-Urteil ECLI "EU:C:2018:388"), kann aber auch auf andere Werbekanäle wie Instagram, Twitter, etc. umgemünzt werden. Die Auswirkungen dieses Urteils auf die Praxis sind noch offen. Es empfiehlt sich aber jedenfalls eine Datenschutzerklärung auf diesen Werbekanälen zu integrieren. Es kann dabei beispielsweise so vorgegangen werden: Bei Facebook kann zB unter "Info" ein Link zur Datenschutzerklärung untergebracht werden. Dabei sollte in der Datenschutzerklärung auf die Zwecke und den Umfang der Facebook-Nutzung durch das Unternehmen hingewiesen werden. Für die Nutzung der Daten durch Facebook kann auf die Datenrichtlinie von Facebook verwiesen werden.
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	Datenschutzerklärung ist in allen Kanälen integriert

Maßnahme:	**M_DSMS_023 Zugang zur Datenschutzerklärung für Mitarbeiter schaffen**
OrgEH:	Personalabteilung TeSA (TeSA_PER)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Mitarbeiter sollten im Zuge der Einstellung und der regelmäßigen Datenschutz-Schulung über die Verarbeitung sie betreffender personenbezogener Daten informiert werden und in weiterer Folge Zugriff zur für sie relevanten Datenschutzerklärung haben. Dies kann zB durch Aushändigen einer Kopie oder Verweis auf ein Dokument in einem jederzeit zugänglichen Ordner (online/offline) oder durch Zugriff über ein Intranet erfolgen.
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	an alle kommunziert und am Z-Laufwerk jederzeit abrufbar

Maßnahme:	**M_DSMS_032 Hinweis auf Beschwerderecht in Datenschutzerklärungen**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Sämtliche Datenschutzerklärungen sind dahingehend zu überprüfen, ob der Hinweis auf das Beschwerderecht bei einer Aufsichtsbehörde enthalten ist. Jede betroffene Person hat das Recht, sich bei einer Aufsichtsbehörde zu beschweren, wenn sie der Ansicht ist, dass eine Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt (Art 77).
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	ist aufgenommen - aktualisierte Erklärung im Anhang

Maßnahme:	**M_DSMS_039 Datenschutzerklärung für Mitarbeiter und Datenschutzrichtlinie in Onboarding-Prozess einbinden**
OrgEH:	Personalabteilung TeSA (TeSA_PER)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Die Datenschutzerklärung für Mitarbeiter und die Datenschutzrichtlinie muss in die Willkommensmappe für neue Mitarbeiter integriert werden und fixer Bestandteil des Onboarding-Prozesses sein
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	ist in Willkommensmappe integriert.

Art. 15 Auskunftsrecht der betroffenen Person

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_015 Bearbeitung von Betroffenenanfragen dokumentieren**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Dokumentieren Sie für jede Betroffenenanfrage insbesondere folgende Punkte: - Zeitablauf: Eingang der Anfrage, Beantwortung der Anfrage - Identitätsverifizierung bzw. Identifizierungsmaßnahmen - gegebenenfalls Verweigerungsgründe - gesetzte Maßnahmen iZm der Anfrage - Art der Kommunikation Eine ordnungsgemäße Dokumentation kann auch helfen, den Nachweis für exzessive Anfragen zu unterstützen.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	Prozess definiert und kommuniziert

Maßnahme:	**M_DSMS_016 Erstellen eines Daten-Mapping-Systems**
OrgEH:	IT Abteilung TeSA (TeSA_IT)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Um die Anforderungen in Bezug auf die Betroffenenrechte gesetzeskonform erfüllen zu können, sollte der Lebenszyklus personenbezogener Daten im Unternehmen festgestellt werden. Es soll feststellbar sein, wo personenbezogene Daten zugänglich sind (Syteme, Applilkationen, etc.), damit schnell identifiziert werden kann, ob personenbezogene Daten vorhanden sind und wo überall sie vorhanden sind und unter welchen Bedingungen sie vorhanden sind. Weiters soll ersichtlich sein, an wen die Daten übermittelt werden, um die Empfänger der Daten leicht ermitteln zu können. Folgendes ist zu dokumentieren: Datenflüsse, Datentransfers zwischen Systemen und Kategorisierung von Systemen nach den Datentransfers. Über eine Datenlandkarte (Daten-Mapping) sollen alle zu einer Person vorliegenden Daten applikationsübergreifend vollständig und lückenlos dargestellt werden. Jedes Datenobjekt kann so mit den Verarbeitungstätigkeiten und rechtlichen Grundlagen sowie den Verarbeitungszwecken verknüpft werden. Im Zuge eines Löschungsbegehrens kann so sichergestellt werden, dass die Daten auf allen Systemen gelöscht werden.
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	fertiggestellt

Maßnahme:	**M_DSMS_017 Musterschreiben Recht auf Auskunft**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Um ein Auskunftsbegehren vollständig und fristgerecht zu beantworten, sollten Musterschreiben vorbereitet werden, die nur mehr an die spezielle Betroffenenanfrage angepasst werden müssen. Ein solches Musterschreiben kann vorgefertigte Textbausteine enthalten, die grundsätzlich folgende Szenarien und Inhalte abdecken sollten: - Hinweis, wenn begründete Zweifel an der Identität der betroffenen Person bestehen (mit Aufforderung zum Identitätsnachweis) - Hinweis auf Fristverlängerung (inkl. Begründung) - Negativauskunft (wenn keine personenbezogenen Daten verarbeitet werden) - Positivauskunft (wenn personenebezogene Daten verarbeitet werden) mit einer Aufstellung der verarbeiteten personenbezogenen Daten, sowie der zusätzlichen in Art 15 Abs 1 geforderten Informationen -> Zwecke und Rechtsgrundlagen der Verarbeitung, Empfänger (insb. Empfänger in Drittländern), Speicherdauer, Herkunft der Daten (wenn sie nicht von der betroffenen Person stammen), Bestehen einer automatisierten Entscheidungsfindung (einschließlich Profiling) inkl. Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen, geeignete Garantien iZm Übermittlung in Drittländer - Information über das Bestehen eines Rechts auf Berichtigung, Löschung, Einschränkung, Widerspruch - Information über Beschwerderecht bei einer Aufsichtsbehörde - Begründung für etwaige Auskunftsverweigerung (inkl. Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde bzw. auf Möglichkeit eines gerichtlichen Rechtsbehelfs) - Begründung für etwaige Kostenersatzforderung (gem. Art 15 Abs 3 oder Art 12 Abs 5 lit a)
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	erstellt

Maßnahme:	**M_DSMS_019 Eingriff in die Rechte und Freiheiten anderer Personen prüfen**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Es soll ein Prozess eingeführt werden, mit dem überprüft wird, ob die Erfüllung eines Betroffenenbegehrens in die Rechte und Freiheiten anderer Personen eingreift.
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	erledigt - siehe Verfahrensanweisung

Abschnitt 3 Berichtigung und Löschung

Art. 16 Recht auf Berichtigung

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_015 Bearbeitung von Betroffenenanfragen dokumentieren**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Dokumentieren Sie für jede Betroffenenanfrage insbesondere folgende Punkte: - Zeitablauf: Eingang der Anfrage, Beantwortung der Anfrage - Identitätsverifizierung bzw. Identifizierungsmaßnahmen - gegebenenfalls Verweigerungsgründe - gesetzte Maßnahmen iZm der Anfrage - Art der Kommunikation Eine ordnungsgemäße Dokumentation kann auch helfen, den Nachweis für exzessive Anfragen zu unterstützen.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	Prozess definiert und kommuniziert

Art. 17 Recht auf Löschung („Recht auf Vergessenwerden“)

Offene Maßnahmen:

Maßnahme:	**M_DSMS_030 Implementieren von Sperrmechanismen**
OrgEH:	IT Abteilung TeSA (TeSA_IT)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Personenbezogene Daten, die für den Verarbeitungszweck nicht mehr gebraucht werden, können oftmals nicht sofort gelöscht werden. Entweder ist eine Löschung technisch noch nicht möglich oder gesetzliche Aufbewahrungsfristen sprechen gegen eine Löschung. In diesen Fällen sollte der Zugriff auf diese Daten zumindest gesperrt werden können. Ebenso kann die Einschränkung der Verarbeitung ein Vorübergehendes Sperren von personenbezogenen Daten notwendig machen.
Fortschritt:	0%

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_015 Bearbeitung von Betroffenenanfragen dokumentieren**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Dokumentieren Sie für jede Betroffenenanfrage insbesondere folgende Punkte: - Zeitablauf: Eingang der Anfrage, Beantwortung der Anfrage - Identitätsverifizierung bzw. Identifizierungsmaßnahmen - gegebenenfalls Verweigerungsgründe - gesetzte Maßnahmen iZm der Anfrage - Art der Kommunikation Eine ordnungsgemäße Dokumentation kann auch helfen, den Nachweis für exzessive Anfragen zu unterstützen.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	Prozess definiert und kommuniziert

Art. 18 Recht auf Einschränkung der Verarbeitung

Offene Maßnahmen:

Maßnahme:	**M_DSMS_030 Implementieren von Sperrmechanismen**
OrgEH:	IT Abteilung TeSA (TeSA_IT)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Personenbezogene Daten, die für den Verarbeitungszweck nicht mehr gebraucht werden, können oftmals nicht sofort gelöscht werden. Entweder ist eine Löschung technisch noch nicht möglich oder gesetzliche Aufbewahrungsfristen sprechen gegen eine Löschung. In diesen Fällen sollte der Zugriff auf diese Daten zumindest gesperrt werden können. Ebenso kann die Einschränkung der Verarbeitung ein Vorübergehendes Sperren von personenbezogenen Daten notwendig machen.
Fortschritt:	0%

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_015 Bearbeitung von Betroffenenanfragen dokumentieren**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Dokumentieren Sie für jede Betroffenenanfrage insbesondere folgende Punkte: - Zeitablauf: Eingang der Anfrage, Beantwortung der Anfrage - Identitätsverifizierung bzw. Identifizierungsmaßnahmen - gegebenenfalls Verweigerungsgründe - gesetzte Maßnahmen iZm der Anfrage - Art der Kommunikation Eine ordnungsgemäße Dokumentation kann auch helfen, den Nachweis für exzessive Anfragen zu unterstützen.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	Prozess definiert und kommuniziert

Art. 19 Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_015 Bearbeitung von Betroffenenanfragen dokumentieren**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Dokumentieren Sie für jede Betroffenenanfrage insbesondere folgende Punkte: - Zeitablauf: Eingang der Anfrage, Beantwortung der Anfrage - Identitätsverifizierung bzw. Identifizierungsmaßnahmen - gegebenenfalls Verweigerungsgründe - gesetzte Maßnahmen iZm der Anfrage - Art der Kommunikation Eine ordnungsgemäße Dokumentation kann auch helfen, den Nachweis für exzessive Anfragen zu unterstützen.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	Prozess definiert und kommuniziert

Maßnahme:	**M_DSMS_018 Mitteilung an Empfänger personenbezogener Daten**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Werden personenbezogene Daten iZm Betroffenenrechten berichtigt, gelöscht oder ihre Verarbeitung eingeschränkt, so müssen sämtliche Empfänger, denen die Daten offengelegt wurden, darüber informiert werden. Hierbei ist die Definition des "Empfängers" gem Art 4 Z 9 zu beachten (ein Empfänger muss demnach nicht zwingend ein "Dritter" sein). Es muss somit eine Prozess geschaffen werden, der sicherstellt, dass Empfänger umgehend von einer Berichtigung/Löschung/Einschränkung informiert werden.
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	erledigt- siehe Verfahrensanweisung

Art. 20 Recht auf Datenübertragbarkeit

Offene Maßnahmen:

Maßnahme:	**M_DSMS_029 Interoperable Standards und Formate verwenden**
OrgEH:	IT Abteilung TeSA (TeSA_IT)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Um das Recht auf Datenübertragbarkeit einfach zu ermöglichen, sollten interoperable Standards und Formate verwendet werden, sofern dies möglich ist.
Fortschritt:	0%

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_015 Bearbeitung von Betroffenenanfragen dokumentieren**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Dokumentieren Sie für jede Betroffenenanfrage insbesondere folgende Punkte: - Zeitablauf: Eingang der Anfrage, Beantwortung der Anfrage - Identitätsverifizierung bzw. Identifizierungsmaßnahmen - gegebenenfalls Verweigerungsgründe - gesetzte Maßnahmen iZm der Anfrage - Art der Kommunikation Eine ordnungsgemäße Dokumentation kann auch helfen, den Nachweis für exzessive Anfragen zu unterstützen.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	Prozess definiert und kommuniziert

Abschnitt 4 Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall

Art. 21 Widerspruchsrecht

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_015 Bearbeitung von Betroffenenanfragen dokumentieren**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Dokumentieren Sie für jede Betroffenenanfrage insbesondere folgende Punkte: - Zeitablauf: Eingang der Anfrage, Beantwortung der Anfrage - Identitätsverifizierung bzw. Identifizierungsmaßnahmen - gegebenenfalls Verweigerungsgründe - gesetzte Maßnahmen iZm der Anfrage - Art der Kommunikation Eine ordnungsgemäße Dokumentation kann auch helfen, den Nachweis für exzessive Anfragen zu unterstützen.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	Prozess definiert und kommuniziert

Maßnahme:	**M_DSMS_031 Musterschreiben Recht auf Widerspruch**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Um einen Widerspruch vollständig und fristgerecht zu beantworten, sollten Musterschreiben vorbereitet werden, die nur mehr an die spezielle Betroffenenanfrage angepasst werden müssen. Ein solches Musterschreiben kann vorgefertigte Textbausteine enthalten, die folgende Szenarien und Inhalte abdecken sollten: - Hinweis, wenn begründete Zweifel an der Identität der betroffenen Person bestehen mit Aufforderung zum Identitätsnachweis) - Hinweis auf etwaige Fristverlängerung (inkl. Begründung) - Negativauskunft, falls keine personenbezogenen Daten des Betroffenen verarbeitet werden - Information darüber, dass keine Maßnahmen in Bezug auf den Widerspruch vorgenommen wurden (inkl. der Gründe dafür und dem Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde bzw. auf Möglichkeit eines gerichtlichen Rechtsbehelfs) - bzw. Information darüber, dass Maßnahmen in Bezug auf den Widerspruch vorgenommen wurden - Begründung für etwaige Kostenersatzforderung (gem. Art 12 Abs 5 lit a)
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	ist erledigt - siehe Anhang

Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

Art. 22 Abs. 1 Verbot der automatisierten Entscheidung im Einzelfall

Art. 22 Abs. 2 Erlaubnistatbestand für automatisierte Entscheidungen im Einzelfall

Art. 22 Abs. 2 lit. a Vertragsabschluss / Vertragserfüllung

Art. 22 Abs. 2 lit. b Rechtsvorschriften

Art. 22 Abs. 2 lit. c ausdrückliche Einwilligung

Art. 22 Abs. 3 angemessene Maßnahmen

Art. 22 Abs. 4 Entscheidungen auf Basis besonderer Kategorien personenbezogener Daten

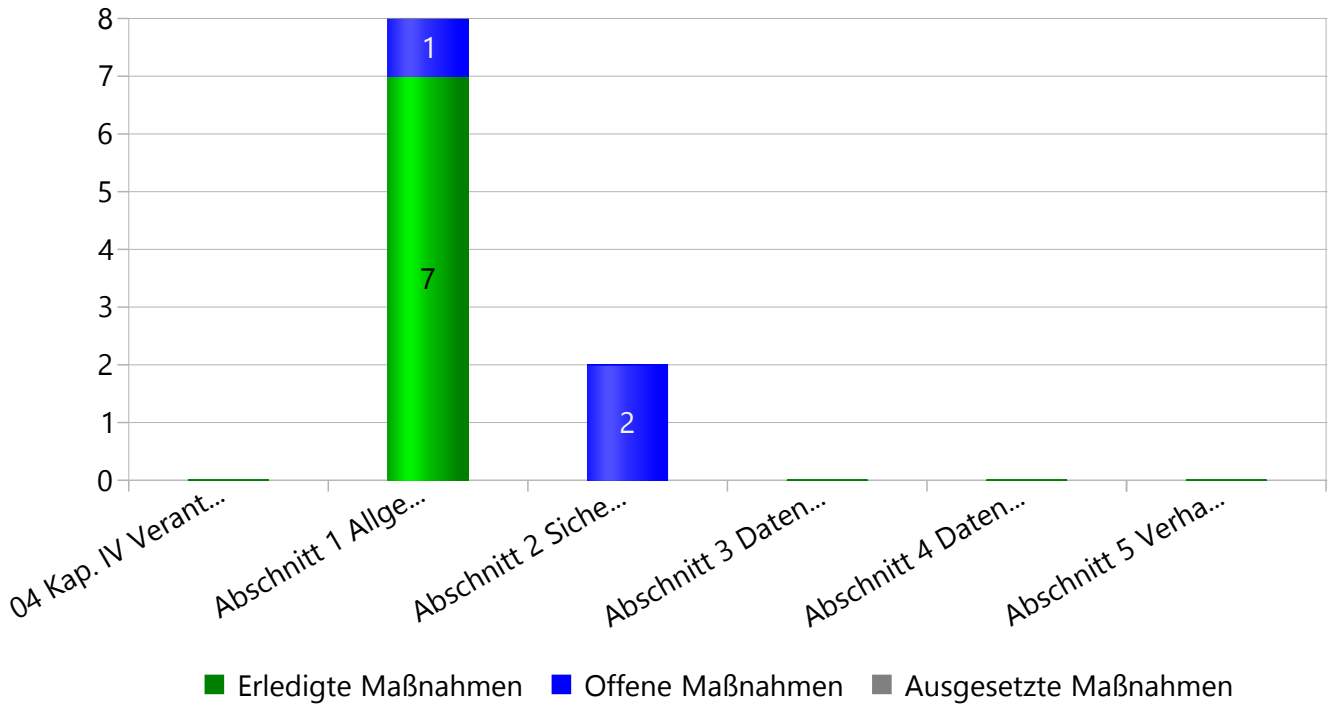
Abschnitt 5 Beschränkungen

Keine zugewiesenen Maßnahmen

Art. 23 Beschränkungen

Keine zugewiesenen Maßnahmen

04 Kap. IV Verantwortlicher und Auftragsverarbeiter



Abschnitt 1 Allgemeine Pflichten

Art. 24 Verantwortung des für die Verarbeitung Verantwortlichen

Offene Maßnahmen:

Maßnahme:	**M_DSMS_028 Vertraulichkeitsvereinbarungen mit Geschäftspartnern abschließen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Geschäftspartner (Lieferanten, Kunden, sonstige Partner), die im Zuge der Zusammenarbeit Zugang zu personenbezogenen Daten haben, sollten auf das Datengeheimnis verpflichtet werden. Darüber hinaus sollten Regelungen zum gemeinsamen Umgang mit personenbezogenen Daten getroffen werden, sofern dies nicht ohnedies zB im Zuge einer allenfalls erforderlichen Auftragsverarbeitervereinbarung erfolgen muss. Die Vertraulichkeitsvereinbarung in Bezug auf personenbezogene Daten kann zB auch in die allgemeine Vertraulichkeitsvereinbarung mit Bezug auf Betriebs- und Geschäftsgeheimnisse integriert werden, sofern sie klar ersichtlich und verständlich ist.
Fortschritt:	0%

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_001 Management Awareness und Committment sicherstellen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Stellen Sie sicher, dass sich das Management der Anforderungen aus der DSGVO und der möglichen Folgen bei Nichterfüllung bewusst ist. Definieren Sie den Bedarf an Ressourcen, der sich aus der Umsetzung der DSGVO in Ihrem Unternehmen ergibt und holen Sie das Committment des Managements ein, diese bereit zu stellen und die Aktivitäten im Zusammenhang mit der Umsetzung zu unterstützen.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	initialer Workshop zu Themenstellungen der DSGVO durchgeführt. Ressourcen soweit definiert und frei gegeben

Maßnahme:	**M_DSMS_002 Verantwortlichkeiten iZm Datenschutz festlegen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Definieren Sie die Rollen im Rahmen des Datenschutzkonzepts und legen Sie die Verantwortlichkeiten zur Erstellung und Umsetzung der einzelnen Prozesse fest. Ermitteln Sie, ob die benötigten Ressourcen innerhalb Ihres Unternehmens vorhanden sind, oder ob Sie auf externe Ressourcen zurückgreifen müssen. Denken Sie dabei ua an Verantwortliche für folgende Prozesse: - Erstellen und Aufrechterhalten des Datenschutzkonzeptes - Erfüllung der Informationspflichten - Umsetzung der Betroffenenrechte - Erstellung und Pflege des Verzeichnisses von Verarbeitungstätigkeiten - Data Breach - Umsetzung technischer und organisatorischer Maßnahmen Überlegen Sie in diesem Zusammenhang auch die Bennennung eines Datenschutzbeauftragten, sofern ein solcher für Ihr Unternehmen nicht ohnehin verpflichtend ist.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	erledigt

Maßnahme:	**M_DSMS_004 Datenschutzrichtlinie erstellen**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Erstellen Sie eine unternehmensspezifische Datenschutzrichtlinie, die zumindest folgende Punkte regelt: - rechtliche Rahmenbedinungen im Unternehmen - die wesentlichen Vorgaben zu den Datenschutzgrundsätzen (Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung und Speicherbegrenzung, Richtigkeit, Integrität und Vertraulichkeit) - grundsätzliche technische und organisatorische Maßnahmen zur Sicherstellung des Datenschutzes - generelle unternehmensinterne Regeln zum Datenschutz
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	Richtlinie erstellt

Maßnahme:	**M_DSMS_005 Dokumentation und Kommunikation der Datenschutzrichtlinie**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Die Datenschutzrichtlinie sollte regelmäßig in aktueller Fassung an alle Mitarbeiter und sonstige relevante Interessensgruppen kommuniziert werden. Es sollte jederzeit ein Zugriff auf die aktuelle Fassung ermöglicht werden.
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	Richtlinie kommuniziert.

Maßnahme:	**M_DSMS_016 Erstellen eines Daten-Mapping-Systems**
OrgEH:	IT Abteilung TeSA (TeSA_IT)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Um die Anforderungen in Bezug auf die Betroffenenrechte gesetzeskonform erfüllen zu können, sollte der Lebenszyklus personenbezogener Daten im Unternehmen festgestellt werden. Es soll feststellbar sein, wo personenbezogene Daten zugänglich sind (Syteme, Applilkationen, etc.), damit schnell identifiziert werden kann, ob personenbezogene Daten vorhanden sind und wo überall sie vorhanden sind und unter welchen Bedingungen sie vorhanden sind. Weiters soll ersichtlich sein, an wen die Daten übermittelt werden, um die Empfänger der Daten leicht ermitteln zu können. Folgendes ist zu dokumentieren: Datenflüsse, Datentransfers zwischen Systemen und Kategorisierung von Systemen nach den Datentransfers. Über eine Datenlandkarte (Daten-Mapping) sollen alle zu einer Person vorliegenden Daten applikationsübergreifend vollständig und lückenlos dargestellt werden. Jedes Datenobjekt kann so mit den Verarbeitungstätigkeiten und rechtlichen Grundlagen sowie den Verarbeitungszwecken verknüpft werden. Im Zuge eines Löschungsbegehrens kann so sichergestellt werden, dass die Daten auf allen Systemen gelöscht werden.
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	fertiggestellt

Maßnahme:	**M_DSMS_025 Datenschutzschulung für Mitarbeiter**
OrgEH:	Personalabteilung TeSA (TeSA_PER)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Mitarbeiter sollten regelmäßig hinsichtlich Datenschutz geschult werden. Neben allgemeinen Inhalten, die alle Mitarbeiter betreffen wie zB: - Datenschutzrichtlinie - Vertraulichkeitsvereinbarungen - Datenschutzerklärung für Mitarbeiter sollten auch bereichsspezifische Informationen im Umgang mit personenbezogenen Daten thematisiert werden. Die Schulungen müssen hinsichtlich Inhalt und Durchführung nachweislich dokumentiert werden
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittsmeldung:	Alle Mitarbeiter initial mit den neuen Unterlagen geschult. Jährliche Auffrischung bereits geplant

Maßnahme:	**M_DSMS_026 Vertraulichkeitsvereinbarungen mit Mitarbeitern abschließen**
OrgEH:	Personalabteilung TeSA (TeSA_PER)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Mitarbeiter müssen auf das Datengeheimnis verpflichtet werden, sofern sie nicht ohnedies einer gesetzlichen Verschwiegenheitspflicht unterliegen . Dies kann auf mehre Arten erfolgen, zB: - Teil des Dienstvertrages - separate Vertraulichkeitserklärung (eventuell gemeinsam mit einer generellen Geheimhaltungsvereinbarung) Die Mitarbeiter sollten jedenfalls ausdrücklich auf das Datengeheimnis hingewiesen werden und im Zuge regelmäßiger Datenschutzschulungen darauf hingewiesen werden.
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittsmeldung:	mit allen MAs Vereinbarung getroffen

Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Art. 25 Abs. 1 Privacy by Design

Art. 25 Abs. 2 Privacy by Default

Art. 26 Gemeinsam für die Verarbeitung Verantwortliche

Art. 26 Abs. 1 Vereinbarung

Art. 26 Abs. 2 Funktionen und Beziehungen

Art. 26 Abs. 3 Geltendmachung von Rechten

Art. 27 Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern

Art. 28 Auftragsverarbeiter

Art. 29 Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Art. 30 Verzeichnis von Verarbeitungstätigkeiten

Art. 31 Zusammenarbeit mit der Aufsichtsbehörde

Abschnitt 2 Sicherheit personenbezogener Daten

Offene Maßnahmen:

Maßnahme:	**M_DSMS_036 Nutzung diverser Social-Media-Kanäle überdenken**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	einige Social-Media-Kanäle sind datenschutzrechtliche bedenklich. Kanäle, die nicht primär genutzt werden, sollten aussortiert werden und für die restlichen, die von hoher Relevanz sind, muss ggf. ein geeignetes Verfahren zur Wahrung des Datenschutzes erarbeitet werden. Dabei sind insbesondere die Informationspflichten zu beachten.
Fortschritt:	0%

Art. 32 Sicherheit der Verarbeitung

Offene Maßnahmen:

Maßnahme:	**M_DSMS_034 Vertraulichkeit, Verfügbarkeit und Integrität personenbezogener Daten sicherstellen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Max Mustermann
Beschreibung:	Setzen Sie Maßnahmen um, die die Vertraulichkeit, Verfügbarkeit und Integrität personenbezogener Daten sicherstellen. Sehen Sie dazu genauere Anweisungen im Kapitel "Technische und Organisatorische Maßnahmen" in dieser Wissensdatenbank zur DSGVO und beachten Sie auch Vorgaben aus dem Informationssicherheitsmanagement (zB auch die Wisssensdatenbank zur Umsetzung der ISO 27001). Mit den bereits gesetzten Maßnahmen im ISMS abgleichen.
Fortschritt:	0%

Art. 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Art. 34 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

Abschnitt 3 Datenschutz-Folgenabschätzung und vorherige Konsultation

Keine zugewiesenen Maßnahmen

Art. 35 Datenschutz-Folgenabschätzung

Keine zugewiesenen Maßnahmen

Art. 36 Vorherige Konsultation

Keine zugewiesenen Maßnahmen

Abschnitt 4 Datenschutzbeauftragter

Keine zugewiesenen Maßnahmen

Art. 37 Benennung eines Datenschutzbeauftragten

Keine zugewiesenen Maßnahmen

Art. 38 Stellung des Datenschutzbeauftragten

Keine zugewiesenen Maßnahmen

Art. 39 Aufgaben des Datenschutzbeauftragten

Keine zugewiesenen Maßnahmen

Abschnitt 5 Verhaltensregeln und Zertifizierung

Keine zugewiesenen Maßnahmen

Art. 40 Verhaltensregeln

Keine zugewiesenen Maßnahmen

Art. 41 Überwachung der genehmigten Verhaltensregeln

Keine zugewiesenen Maßnahmen

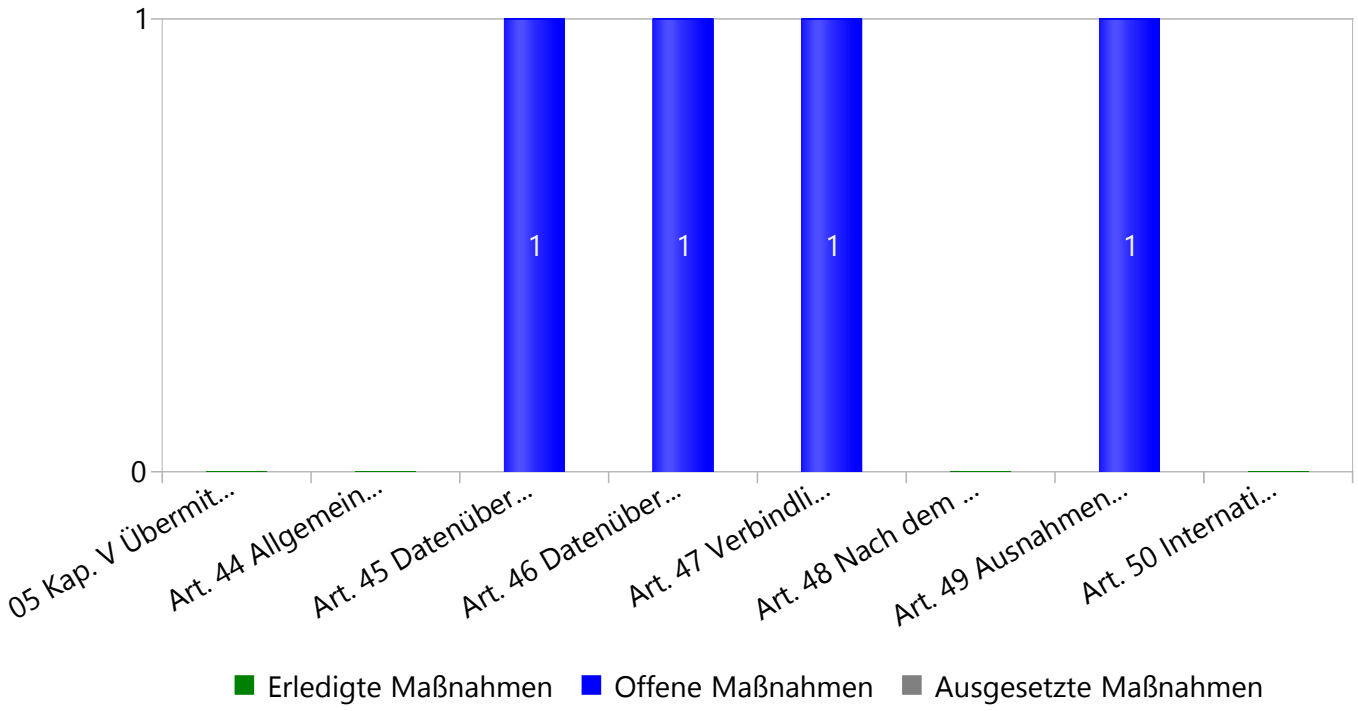
Art. 42 Zertifizierung

Keine zugewiesenen Maßnahmen

Art. 43 Zertifizierungsstellen

Keine zugewiesenen Maßnahmen

05 Kap. V Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen



Art. 44 Allgemeine Grundsätze der Datenübermittlung

Keine zugewiesenen Maßnahmen

Art. 45 Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

Offene Maßnahmen:

Maßnahme:	**M_DSMS_035 Datenübermittlungen in Drittländer DSGVO-konform durchführen**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Überprüfen Sie, ob in Ihrem Unternehmen personenbezogene Daten an Unternehmen/Einrichtungen/ Institutionen in Drittländer übertragen werden. Wenn dies der Fall ist, stellen Sie sicher, dass im Drittland ein der DSGVO entsprechendes Datenschutzniveau herrscht. Dieses kann nachgewiesen werden durch: - einen Angemessenheitsbeschluss der EU Kommission - das Vorhandensein geeigneter Garantien, zB in Form von verbindlichern internern Datenschutzvorschriften oder von der Kommission erlassenen oder genehmigten Standardvertragsklauseln (gem. Art 46 und 47) - das Bestehen eines Ausnahmetatbestands gemäß Art 49 (zB ausdrückliche Einwilligung der betroffenen Person, Erfüllung eines Vertrages auf Antrag der betroffenen Person, etc.)
Fortschritt:	0%

Art. 46 Datenübermittlung vorbehaltlich geeigneter Garantien

Offene Maßnahmen:

Maßnahme:	**M_DSMS_035 Datenübermittlungen in Drittländer DSGVO-konform durchführen**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Überprüfen Sie, ob in Ihrem Unternehmen personenbezogene Daten an Unternehmen/Einrichtungen/ Institutionen in Drittländer übertragen werden. Wenn dies der Fall ist, stellen Sie sicher, dass im Drittland ein der DSGVO entsprechendes Datenschutzniveau herrscht. Dieses kann nachgewiesen werden durch: - einen Angemessenheitsbeschluss der EU Kommission - das Vorhandensein geeigneter Garantien, zB in Form von verbindlichern internern Datenschutzvorschriften oder von der Kommission erlassenen oder genehmigten Standardvertragsklauseln (gem. Art 46 und 47) - das Bestehen eines Ausnahmetatbestands gemäß Art 49 (zB ausdrückliche Einwilligung der betroffenen Person, Erfüllung eines Vertrages auf Antrag der betroffenen Person, etc.)
Fortschritt:	0%

Art. 47 Verbindliche interne Datenschutzvorschriften

Offene Maßnahmen:

Maßnahme:	**M_DSMS_035 Datenübermittlungen in Drittländer DSGVO-konform durchführen**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Überprüfen Sie, ob in Ihrem Unternehmen personenbezogene Daten an Unternehmen/Einrichtungen/ Institutionen in Drittländer übertragen werden. Wenn dies der Fall ist, stellen Sie sicher, dass im Drittland ein der DSGVO entsprechendes Datenschutzniveau herrscht. Dieses kann nachgewiesen werden durch: - einen Angemessenheitsbeschluss der EU Kommission - das Vorhandensein geeigneter Garantien, zB in Form von verbindlichern internern Datenschutzvorschriften oder von der Kommission erlassenen oder genehmigten Standardvertragsklauseln (gem. Art 46 und 47) - das Bestehen eines Ausnahmetatbestands gemäß Art 49 (zB ausdrückliche Einwilligung der betroffenen Person, Erfüllung eines Vertrages auf Antrag der betroffenen Person, etc.)
Fortschritt:	0%

Art. 48 Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung

Keine zugewiesenen Maßnahmen

Art. 49 Ausnahmen für bestimmte Fälle

Offene Maßnahmen:

Maßnahme:	**M_DSMS_035 Datenübermittlungen in Drittländer DSGVO-konform durchführen**
OrgEH:	Rechtsabteilung TeSA (TeSA_RE)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Überprüfen Sie, ob in Ihrem Unternehmen personenbezogene Daten an Unternehmen/Einrichtungen/ Institutionen in Drittländer übertragen werden. Wenn dies der Fall ist, stellen Sie sicher, dass im Drittland ein der DSGVO entsprechendes Datenschutzniveau herrscht. Dieses kann nachgewiesen werden durch: - einen Angemessenheitsbeschluss der EU Kommission - das Vorhandensein geeigneter Garantien, zB in Form von verbindlichern internern Datenschutzvorschriften oder von der Kommission erlassenen oder genehmigten Standardvertragsklauseln (gem. Art 46 und 47) - das Bestehen eines Ausnahmetatbestands gemäß Art 49 (zB ausdrückliche Einwilligung der betroffenen Person, Erfüllung eines Vertrages auf Antrag der betroffenen Person, etc.)
Fortschritt:	0%

Art. 50 Internationale Zusammenarbeit zum Schutz personenbezogener Daten

Keine zugewiesenen Maßnahmen

06 Kap. VI Unabhängige Aufsichtsbehörden

Art. 51 Aufsichtsbehörde

Keine zugewiesenen Maßnahmen

Art. 52 Unabhängigkeit

Keine zugewiesenen Maßnahmen

Art. 53 Allgemeine Bedingungen für die Mitglieder der Aufsichtsbehörde

Keine zugewiesenen Maßnahmen

Art. 54 Errichtung der Aufsichtsbehörde

Keine zugewiesenen Maßnahmen

Art. 55 Zuständigkeit

Keine zugewiesenen Maßnahmen

Art. 56 Zuständigkeit der federführenden Aufsichtsbehörde

Keine zugewiesenen Maßnahmen

Art. 57 Aufgaben

Keine zugewiesenen Maßnahmen

Art. 58 Befugnisse

Keine zugewiesenen Maßnahmen

Art. 59 Tätigkeitsbericht

Keine zugewiesenen Maßnahmen

07 Kap. VII Zusammenarbeit und Kohärenz

Art. 60 Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den anderen betroffenen Aufsichtsbehörden

Keine zugewiesenen Maßnahmen

Art. 61 Gegenseitige Amtshilfe

Keine zugewiesenen Maßnahmen

Art. 62 Gemeinsame Maßnahmen der Aufsichtsbehörden

Keine zugewiesenen Maßnahmen

Art. 63 Kohärenzverfahren

Keine zugewiesenen Maßnahmen

Art. 64 Stellungnahme Ausschusses

Keine zugewiesenen Maßnahmen

Art. 65 Streitbeilegung durch den Ausschuss

Keine zugewiesenen Maßnahmen

Art. 66 Dringlichkeitsverfahren

Keine zugewiesenen Maßnahmen

Art. 67 Informationsaustausch

Keine zugewiesenen Maßnahmen

Art. 68 Europäischer Datenschutzausschuss

Keine zugewiesenen Maßnahmen

Art. 69 Unabhängigkeit

Keine zugewiesenen Maßnahmen

Art. 70 Aufgaben des Ausschusses

Keine zugewiesenen Maßnahmen

Art. 71 Berichterstattung

Keine zugewiesenen Maßnahmen

Art. 72 Verfahrensweise

Keine zugewiesenen Maßnahmen

Art. 73 Vorsitz

Keine zugewiesenen Maßnahmen

Art. 74 Aufgaben des Vorsitzes

Keine zugewiesenen Maßnahmen

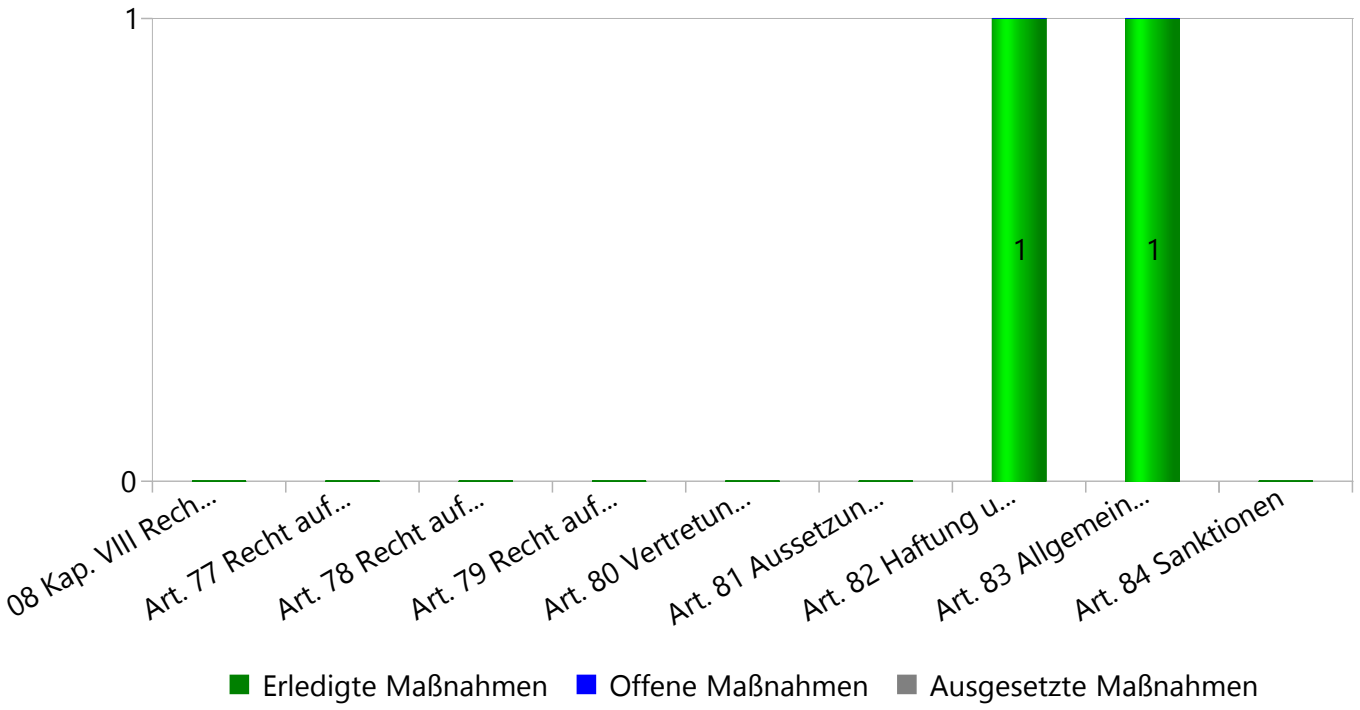
Art. 75 Sekretariat

Keine zugewiesenen Maßnahmen

Art. 76 Vertraulichkeit

Keine zugewiesenen Maßnahmen

08 Kap. VIII Rechtsbehelfe, Haftung und Sanktionen



Art. 77 Recht auf Beschwerde bei einer Aufsichtsbehörde

Keine zugewiesenen Maßnahmen

Art. 78 Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde

Keine zugewiesenen Maßnahmen

Art. 79 Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter

Keine zugewiesenen Maßnahmen

Art. 80 Vertretung von betroffenen Personen

Keine zugewiesenen Maßnahmen

Art. 81 Aussetzung des Verfahrens

Keine zugewiesenen Maßnahmen

Art. 82 Haftung und Recht auf Schadenersatz

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_001 Management Awareness und Committment sicherstellen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Stellen Sie sicher, dass sich das Management der Anforderungen aus der DSGVO und der möglichen Folgen bei Nichterfüllung bewusst ist. Definieren Sie den Bedarf an Ressourcen, der sich aus der Umsetzung der DSGVO in Ihrem Unternehmen ergibt und holen Sie das Committment des Managements ein, diese bereit zu stellen und die Aktivitäten im Zusammenhang mit der Umsetzung zu unterstützen.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	initialer Workshop zu Themenstellungen der DSGVO durchgeführt. Ressourcen soweit definiert und frei gegeben

Art. 83 Allgemeine Bedingungen für die Verhängung von Geldbußen

Erledigte Maßnahmen:

Maßnahme:	**M_DSMS_001 Management Awareness und Committment sicherstellen**
OrgEH:	Team Secure AG (TeSA)
Verantwortliche(r):	Tom Leisch
Beschreibung:	Stellen Sie sicher, dass sich das Management der Anforderungen aus der DSGVO und der möglichen Folgen bei Nichterfüllung bewusst ist. Definieren Sie den Bedarf an Ressourcen, der sich aus der Umsetzung der DSGVO in Ihrem Unternehmen ergibt und holen Sie das Committment des Managements ein, diese bereit zu stellen und die Aktivitäten im Zusammenhang mit der Umsetzung zu unterstützen.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittsmeldung:	initialer Workshop zu Themenstellungen der DSGVO durchgeführt. Ressourcen soweit definiert und frei gegeben

Art. 84 Sanktionen

Keine zugewiesenen Maßnahmen

09 Kap. IX Vorschriften für besondere Verarbeitungssituationen

Art. 85 Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit

Keine zugewiesenen Maßnahmen

Art. 86 Verarbeitung und Zugang der Öffentlichkeit zu amtlichen Dokumenten

Keine zugewiesenen Maßnahmen

Art. 87 Verarbeitung der nationalen Kennziffer

Keine zugewiesenen Maßnahmen

Art. 88 Datenverarbeitung im Beschäftigungskontext

Keine zugewiesenen Maßnahmen

Art. 89 Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

Keine zugewiesenen Maßnahmen

Art. 90 Geheimhaltungspflichten

Keine zugewiesenen Maßnahmen

Art. 91 Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften

Keine zugewiesenen Maßnahmen

10 Kap. X Delegierte Rechtsakte und Durchführungsrechtakte

Art. 92 Ausübung der Befugnisübertragung

Keine zugewiesenen Maßnahmen

Art. 93 Ausschussverfahren

Keine zugewiesenen Maßnahmen

11 Kap. XI Schlussbestimmungen

Art. 94 Aufhebung der Richtlinie 95/46/EG

Keine zugewiesenen Maßnahmen

Art. 95 Verhältnis zur Richtlinie 2002/58/EG

Keine zugewiesenen Maßnahmen

Art. 96 Verhältnis zu bereits geschlossenen Übereinkünften

Keine zugewiesenen Maßnahmen

Art. 97 Berichte der Kommission

Keine zugewiesenen Maßnahmen

Art. 98 Überprüfung anderer Rechtsakte der Union zum Datenschutz

Keine zugewiesenen Maßnahmen

Art. 99 Inkrafttreten und Anwendung

Keine zugewiesenen Maßnahmen