Bußgeldtabelle International DSGVO / Datenschutzrecht alt & neu - Jahre 2018 / 2019 – unvollständig

Datum	Behörde	Land	Bußgeld (in Euro)	Bußgeld (in Landeswährung)	Vermutlich Verstoß Gegen (DS-GVO)	Verantwortlicher	Sachverhalt	Online-Fundstelle(n)		
24.7.19	FTC	USA	4.485.475.000 €	5.000.000.000 $		Facebook	Auch wenn es bei dem Vergleich zwischen FTC und Facebook nicht um ein Bußgeld nach DSGVO geht, wurden ähnliche Datenschutzverstöße geahndet: Durch den Cambridge Analytica-Skandal waren Zugriffe Dritter auf persönliche Daten bekannt geworden, die dann zur gezielten Stimmungsmache genutzt wurden. Facebook hatte zudem Fehlinformationen zur Nutzung der Gesichtserkennung bereitgestellt und zur Sicherheit hinterlegte Mobilfunknummern anderweitig zu Werbezwecken verwendet. Facebook verpflichtete sich im Rahmen des Vergleichs zu einem transparenteren Umgang mit Kundendaten und zur Implementierung neuer Strukturen zur Sicherung der Privatheit der persönlichen Daten.	Link	Link	Link
8.7.19	ICO	Großbritannien	204.000.000 €	(noch nicht final) 183.390.000 £	Art. 32	British Airways	Die Kreditkarten- und Adressdaten von ca. 500.000 Kunden waren wegen unzureichenden Sicherheitsvorkehrungen durch eine Umleitung auf eine andere Seite gehackt worden. Das Datenleck hatte British Airways selbst gemeldet.	Link	Link	
9.7.19	ICO	Großbritannien	110.000.000 €	(noch nicht final) 99.200.396 £	Art. 32	Marriott International, Inc.	Unbefugte hatten Zugriff auf Daten von 339.000.000 Gästen, davon ca. 30.000.000 aus EU-Ländern. Das Datenleck soll auf ungenügende Sicherheitsvorkehrungen nach der Übernahme von Starwood (2016) zurückzuführen sein. Marriott meldete das Leck selbst.	Link	Link	
24.7.19	SEC	USA	89.709.500 €	100.000.000 $	-	Facebook	Auch wenn es bei dem Vergleich zwischen SEC und Facebook nicht um ein Bußgeld nach DSGVO geht, waren ähnliche Datenschutzverstöße betroffen: Durch den Cambridge Analytica-Skandal waren Zugriffe Dritter auf persönliche Daten bekannt geworden, die dann zur gezielten Stimmungsmache genutzt wurden. Das SEC ahndete das Leugnen Facebooks, dass die Datensicherheit gegenüber Dritten nicht gewährleistet sei, als ihnen das Datenleck längst bekannt war.	Link	Link	Link
21.1.19	CNIL	Frankreich	50.000.000 €	-	Art. 4 Nr.11, 5, 6, 13, 14	Google LLC	Google verstieß nach Ansicht des CNIL gegen zahlreiche Datenschutzgrundsätze wie das Transparenzgebot und die Zweckbindung, da z.B. für personalisierte Werbung mit einem vorangekreuzten Kästchen ohne Einwilligung Daten gesammelt wurden oder Einwilligungen für mehr als einen Zweck gebündelt eingeholt wurden. Zudem seien an vielen Stellen die Informationen für Kunden schwer verständlich oder unklar.	Link	Link	Link
28.8.19	CPDP bzw. KZLD	Bulgarien	2.600.000 €	5.100.000 BGN	Art. 32	Nationale Steuerbehörde (NRA bzw. NAP)	Die Datenschutzaufsichtsbehörde verhängte das Bußgeld gegen die NRA, weil aufgrund mangelnder technischer und organisatorischer Maßnahmen die Daten von über 6 Mio. lebenden und verstorbenen Personen gestohlen und im Internet veröffentlicht worden waren. Zusätzlich hat die Steuerbehörde 6 Monate Zeit, um Maßnahmen zur Verbesserung der Sicherheit umzusetzen und um eine Risikoanalyse und eine neue Datenschutzfolgenabschätzung für jedes System durchzuführen. Bezüglich der Beschwerden, die weiterhin bei der Aufsichtsbehörde eingingen, merkte diese an, dass mit der Überprüfung und der Anordnung der Maßnahmen und des Bußgelds das Verfahren abgeschlossen sei und nach dem Grundsatz „ne bis in idem" weitergehende zivilrechtliche Einzelansprüche nur noch gerichtlich verfolgbar seien, dies aber keiner erneuten Überprüfung der Behörde bedürfe.	Link	Link	
28.6.19	Garante	Italien	1.000.000 €	-	-	Facebook	Obwohl das Bußgeld nach altem Recht verhängt wurde, sind dieselben Datenschutzgrundsätze betroffen. Durch den Cambridge Analytica-Skandal wurde der Zugriff Dritter auf persönliche Daten von Facebook-Nutzern bekannt, darunter befanden sich auch die Daten von über 200.000 Italienern. Die Garante rügte den intransparenten Umgang mit den Daten, die fehlende Legitimation (Einwilligung) zur Nutzung und die unkooperative Haltung gegenüber der Aufsichtsbehörde. Unter der DSGVO hätte dass Bußgeld erheblich höher ausfallen können.	Link	Link	
28.8.19	CPDP bzw. KZLD	Bulgarien	511.000 €	1.000.000 BGN	Art. 32	„Banka DSK" EAD (DSK Bank)	Die Aufsichtsbehörde verhängte das Bußgeld gegen die Bank, da aufgrund mangelnder technischer und organisatorischer Maßnahmen die Daten von über 30.000 Kunden und unzähligen verbundenen Personen (z.B. Ehepartnern und Kindern) unbefugten Dritten zugänglich waren. Da unzählige Personen betroffen waren und in vereinzelten Fällen sogar Krankheitsdaten als besonders sensible Daten darunter waren (z.B. Krankheit als Grund für verminderte Erwerbsfähigkeit bei einem Kreditantrag aufgeführt), fiel das Bußgeld besonders hoch aus.	Link		
16.7.19	AP	Niederlande	460.000 €	-	Art. 32	HagaZiekenhuis (Haga-Krankenhaus)	Das Krankenhaus wurde mit dem Bußgeld belegt, da wichtige Sicherheits-vorkehrungen zum Schutz der Krankendaten vor dem Zugang Unbefugter nicht getroffen worden waren, wie z.B. die Überprüfung von Protokolldateien und die Zwei-Faktoren-Authentifizierung. Die Mängel kamen heraus, als mehrere Mitarbeiter, die hierzu unbefugt waren, Einsicht in die Krankenakte einer Reality-TV-Persönlichkeit nahmen. Das Krankenhaus bekam außerdem ein Ultimatum, um hinreichende Sicherheitsvorkehrungen zu implementieren. Bei Ablauf drohen weitere Bußgelder.	Link	Link	
17.7.18	CNPD	Portugal	400.000 €	-	Art. 5 I f, 32	Centro Hospitalar Barreiro Montijo (Krankenhaus)	Das Krankenhaus hatte keine hinreichenden Sicherheitsvorkehrungen zum Schutz der Krankendaten getroffen. Es kam heraus, dass mehr als 3x so viele Ärzte-Nutzerprofile registriert waren wie Ärzte dort arbeiteten und auch Techniker Zugang zu besonders zu schützenden Daten hatten. Die Ärzte hatten zudem ungeachtet ihrer Spezialisierung unbegrenzten Zugang zu allen Patientenakten.	Link	Link	
28.5.19	CNIL	Frankreich	400.000 €	-	Art. 5, 32	Sergic (Immobiliendienstleister)	Daten von abgelehnten Mietkandidaten wurden nach der Überprüfung weiter gespeichert und kein Datum für die Löschung festgelegt. Auf der Webseite von Sergic war ein Zugang durch Unbefugte zu sensiblen personenbezogenen Daten wie z.B. Ausweiskopien möglich. Die Überprüfung durch die CNIL nach Beschwerde eines Kunden ergab zudem, dass die Schwachstelle dem Unternehmen seit Monaten bekannt gewesen und dennoch nichts unternommen worden war.	Link	Link	
11.6.19	AEPD	Spanien	250.000 €	-	Art. 5 I a, 7 III	La Liga (Profi-Fußball-Liga)	Um Schaden durch illegale Übertragungen der Pay-TV-Spiele in Sportbars vorzubeugen, hatte LaLiga mit ihrer App die Handy-Mikrofone der etwa 10 Millionen Nutzer aktiviert, um so durch kurze Aufnahmen illegale Übertragungsorte identifizieren zu können. Dass die Einwilligung in den Zugriff auf Mikrofondaten auch zur Überwachung dienen sollte, war den Nutzern nicht bekannt und eine Widerrufsmöglichkeit für diese Funktion nicht transparent genug. LaLiga verteidigte sich damit, dass nur während der Spielzeiten für kurze Ausschnitte das Mikrofon eingeschaltet würde, um Übereinstimmungen mit den laufenden Spielen zu erkennen. Persönliche Gespräche der Betroffenen würden zu keiner Zeit mitgeschnitten.	Link	Link	Link
15.3.19	UODO	Polen	220.000 €	943.000 PLN	Art. 14	Bisnode AB (Anbieter für digitale Wirtschaftsinformationen)	Das Unternehmen hatte im Fall von über 6 Mio. Personen Daten aus öffentlich zugänglichen Quellen erhoben, ohne diese zu informieren, da sie keine E-Mail-Adressen zur Verfügung hatten und ihnen der finanzielle und organisatorische Aufwand, diese Personen über die vorhandenen Telefonnummern oder Postanschriften zu kontaktieren, zu groß war. Die Aufsichtsbehörde verhängte das Bußgeld in dieser Höhe, da ihrer Ansicht nach das Unternehmen die Informationspflicht bewusst ignoriert hatte und auch keinen Willen zeigte, das Vorgehen zukünftig zu ändern.	Link	Link	
3.6.19	Datatilsynet	Dänemark	200.880 €	1.500.000 DKK	Art. 5 I e	IDdesign A/S (Möbelhersteller)	IDdesign speicherte die Daten von ca. 385.00 Kunden ohne Löschung nach Abschluss von Geschäftsbeziehungen und ohne ein Datum für die Löschung festzulegen und verstieß damit gegen den Grundsatz der Speicherbegrenzung. Bei dem Bußgeld handelt es sich um eine Empfehlung durch die Datatilsynet, das in Dänemark nur ein Gericht verhängen kann.	Link	Link	
25.7.19	CNIL	Frankreich	180.000 €	-	Art. 32	Active Assurances (Auto-Versicherungsanbieter)	Die Aufsichtsbehörde bemängelte die leichte Zugänglichkeit Unbefugter zu Daten (wie kopierten Führerscheinen und Bankverbindungsdaten) auf der Webseite aufgrund organisatorischer Mängel, die z.B. ein Passwort-Management beinhalteten, dass Zugang ohne weitere Authorisierung ermöglichte.	Link	Link	
29.3.19	Datatilsynet	Norwegen	170.000 €	1.600.000 NOK	Art. 5 I f, 32	Stadtverwaltung Bergen	Die Sicherheitsvorkehrungen im Verwaltungssystem der Stadt in Bezug auf 35.000 Nutzerkonten von den Grundschulen waren ungenügend, so dass z.B. Adressen, Geburtsdaten und Schulnoten ohne großen Aufwand von Unbefugten eingesehen werden konnten, sowohl auf der Online-Lernplattform als auch im Schulverwaltungssystem. Ein interner Whistleblower hatte darauf schon zuvor hingewiesen und auch die Aufsichtsbehörde hatte die Gemeinde gewarnt. Besonders erschwerend wurde bei der Bußgeldhöhe berücksichtigt, dass bei den 35.000 ungeschützten Nutzerkonten neben denen der Angestellten auch gerade die der Kinder als besonders schützenswerten Adressaten der DSGVO betroffen waren.	Link	Link	Link

25.3.19	Datatilsynet	Dänemark	160.000 €	(noch nicht final) 1.200.000 DKK	Art. 5 I e	Taxa 4x35 (Taxiunternehmen)	Die Kundennamen wurden regelmäßig nach 2 Jahren gelöscht, die Telefonnummern und Daten zu den Fahrten allerdings für 5 Jahre gespeichert. Bei einer Überprüfung durch die Aufsichtsbehörde wurden über 8 Mio. Datensätze gefunden, die über die notwendige Zeit von 2 Jahren hinaus gespeichert worden waren. Die große Anzahl von ohne legitimen Grund gespeicherten Daten wirkte sich erschwerend auf die Höhe des Bußgelds aus. Dabei handelt es sich nach dänischem Recht zunächst nur um eine Empfehlung, die Verhängung erfolgt dann durch ein Gericht.	Link	Link	
2019	HDPA	Griechenland	150.000 €	-	Art. 5 I a, b, c, 13 I c, 14 I c	Pricewaterhouseco opers Business Solutions SA	Das Unternehmen hatte seine Angestellten Einwilligungen zur Datenverarbeitung unterzeichnen lassen und damit dann auch Daten erhoben, die über das Notwendige hinausgingen. Da sich die Verarbeitung im Arbeitgeber-Arbeitnehmer-Verhältnis aber bereits auf einen legitimen Zweck stützt, kann eine Einwilligung nicht greifen und ein Widerruf wäre wirkungslos. Zudem wäre eine Einwilligung bei dem Ungleichgewicht zwischen Arbeitgeber und Arbeitnehmer nie freiwillig. Darüber wurden die Arbeitnehmer nicht hinreichend informiert, sodass Verstöße gegen das Transparenzgebot, Zweckbindung, Datenminimierung und Informationspflichten vorlagen.	Link	Link	
27.6.19	ANSPDCP	Rumänien	130.000 €	613.912 RON	Art. 5 I c, 25 I	UniCredit Bank S.A.	Das Bußgeld wurde aufgrund unzureichender technischer und organisatorischer Maßnahmen zum generellen Schutz und auch der Minimierung der Kundendaten verhängt. Aufgrund der Mängel hatten z.B. Kunden beim Erhalt von Online-Überweisungen Zugriff auf Daten des Überweisenden.	Link	Link	
23.5.19	NAIH	Ungarn	93.000 €	30.000.000 HUF	Art. 5 I b,c, 5 II, 6, 6 I f	Sziget Kulturális Menedzser Iroda Zártkörűen Működő Részvénytársaság (Organisator des Sziget Festivals)	Der Festival-Organisator hatte ein Check-In System implementiert, das neben einem Foto der Festivalbesucher auch zahlreiche Daten (wie Geburtsdatum) erfasste und auf Chips in Armbändern speicherte. So wollte man Missbrauch wie dem Mehrfachzutritt durch Wechsel eines Armbandes unter mehreren Personen und Sicherheitsbedenken (anlässlich der Bataclan-Ereignisse in Paris) vorbeugen. Auch auf Hinweis der Aufsichtsbehörde, dass eine Einwilligung oder ein legitimer Zweck für die Erhebung der umfassenden Daten und ihrer Speicherung nicht gegeben sei, reagierte der Veranstalter nicht mit Änderungen.	Link	Link	Link
16.5.19	VDAI	Litauen	61.500 €	-	Art. 5, 32, 33	UAB MisterTango (Zahlungsdienstanbieter)	Für zwei Tage waren Daten der Kunden für Unbefugte online einsehbar, dieses Datenleck hatte der Betreiber nicht gemeldet - die Aufsichtsbehörde stellte außerdem fest, dass entgegen dem Grundsatz der Datenminimierung für die Dienstleistung überflüssige Daten gesammelt wurden.	Link	Link	
Aug 19	AEPD	Spanien	60.000 €	-	Art. 6	Avon Cosmetics SAU	Die Aufsichtbehörde verhängte das Bußgeld gegen Avon, weil diese die Daten eines ihrer Vertreter ins Schuldnerregister eintragen ließen, nachdem er für die Produkte nicht zahlte. Der Betroffene war allerdings nie selbst einen Vertrag mit Avon eingegangen, sondern von einem Dritten angemeldet worden. Der Betroffene hatte Avon auch darauf hingewiesen und Löschung seiner Daten aus dem Register gefordert. Obwohl seine Unterschrift mit der im Vertrag nicht übereinstimmte, kam Avon dem nicht nach. Nach Ansicht der Aufsichtsbehörde hätte sich das Unternehmen der Identität seines Schuldners vorher ausreichend versichern müssen und auch die Meldung an das Schuldnerregister gar nicht erst vornehmen dürfen.	Link	Link	Link
2019	AEPD	Spanien	60.000 €	-	Art. 5 I f	Géstion De Cobros, Yo Cobro, SL (Inkassobüro)	Das Inkassobüro sendete wiederholt E-Mails an einen Schuldner, der angeblich einen Mikrokredit nicht zurückgezahlt hatte, allerdings nicht nur an die bei dem Kreditgeber hinterlegten Adressen sondern auch an eine Adresse seines Arbeitsplatzes, zu der auch seine Kollegen Zugang hatten. Die Aufsichtsbehörde berücksichtigte die Dauer und den Umfang des Verstoßes sowie die mangelnde Kooperation bei der Aufklärung erschwerend.	Link		
2019	AEPD	Spanien	60.000 €	-	Art. 5 I f	Endesda Energía XXI, SLU (Energieversorger)	Das Energieunternehmen hatte von dem Endesda-Konto einer Kundin zugunsten eines Dritten abgebucht, gegen den diese eine einstweilige Verfügung erwirkt hatte. Der Dritte hatte seine Daten telefonisch an der Stelle der Daten der Betroffenen eintragen lassen, indem er einfach vorgab, dass die vorhandenen Daten, die ihm für das Konto mitgeteilt wurden, falsch seien. Endesda hat sich gegenüber der Aufsichtsbehörde dazu verpflichtet, die Telefonberater besser im Umgang mit vertraulichen Daten zu schulen, damit die Sicherheitslücke, dass Daten ohne weitere Überprüfung an Anrufer herausgegeben werden, geschlossen wird.	Link		
4.4.19	Garante	Italien	50.000 €	-	Art. 32	Rousseau (Internet-Plattformbetreiber) / Movimento 5 Stelle (5-Sterne-Bewegung)	Die Plattform Rousseau, die mehrere Internetseiten für die Partei Movimento 5 Stelle betreute, war 2017 Opfer eines Hackerangriffs geworden. Daraufhin (nach altem Datenschutz-Recht) verhängte Maßnahmen zur Verbesserung der Sicherheit (z.B. Anonymisierung der Daten beim e-voting), wurden offenbar nicht umgesetzt, was bei einer Überprüfung zu dem Bußgeld nach DSGVO führte. Obwohl die Partei eigentlich die Daten erhob, wurde der Plattform-Betreiber als Verarbeiter der Daten zur Verantwortung gezogen.	Link	Link	Link
Aug 19	DSB	Österreich	50.000 €	(noch nicht final)	Art. 13, 37	Medizinisches Unternehmen	Das Unternehmen war offenbar Informationspflichten nicht nachgekommen und hatte auch keinen Datenschutzbeauftragten bestellt.	Link		
21.3.19	NAIH	Ungarn	35.000 €	11.000.000 HUF	Art. 33, 34	Demokratikus Koalíció (politische Partei)	Die personenbezogenen Daten (Namen, E-Mail-Adressen, Passwörter) von ca. 6.000 Parteimitgliedern und Unterstützern, die auf der Webseite der DK registriert waren, waren in einem anonymen Hackerforum veröffentlicht worden. Die Aufsichtsbehörde belegte, nachdem sie von einem Bürger darauf aufmerksam gemacht worden war, die DK mit dem Bußgeld, da sie versäumt hatte, das Datenleck zu melden und die Betroffenen zu benachrichtigen. Die Partei hatte argumentiert, es sei unnötig gewesen, den Hack zu melden, da es sich nur um veraltete, jahrelang nicht aktualisierte Daten handelte, die betroffen waren. Die NAIH widersprach, da es sich immer noch um ein hohes Sicherheitsrisiko handle, auch wenn seit Jahren keine Aktualisierung der Daten erfolgt war, da die politische Einstellung der Betroffenen sich nicht zwingend geändert habe und öffentlich zugänglich war, ohne dass die Betroffenen davon erfuhren. Zudem rügte die NAIH die veralteten Sicherheitsmaßnahmen auf der Webseite der DK.	Link	Link	
26.2.19	CPDP bzw. KZLD	Bulgarien	27.100 €	53.000 BGN	Art. 5 I a, 6	"T.B." EAD (Telekommunikations-dienstleister)	Ein Kunde wurde ohne sein Wissen oder seine Einwilligung mehrfach beim Prepaid-Service registriert. Nach Überprüfung stellte die Aufsichtsbehörde fest, dass die Unterschrift und Ausweisnummer auf dem Antrag nicht mit denen des Betroffenen übereinstimmten, aber dennoch sein Vertrag ohne Abgleich abgeändert wurde.	Link		
2018	AEPD	Spanien	27.000 €	-	Art. 5 I d	Vodafone Espana	Die Daten eines Kunden wurden auch nach Vertragsauflösung gespeichert und seine Mobilfunknummer zur Zusendung von über 200 Werbe-SMS genutzt. Nach Statement des Mobilfunkanbieters war die Telefonnummer des ehemaligen Kunden fälschlicherweise zu "Testzwecken" freigegeben und in verschiedenen zu anderen Kunden gehörenden Dateien abgespeichert.	Link	Link	Link
13.6.19	CNIL	Frankreich	20.000 €	-	Art. 5 I c, 12, 13, 32	UNIONTRAD COMPANY (Übersetzungsdienstleister)	Die UNIONTRAD COMPANY hatte nach bereits erfolgter Mahnung durch die CNIL bei einer erneuten Überprüfung weiterhin Kameras zur dauerhaften Überwachung der 9 Angestellten installiert. Zu den verarbeiteten Daten stellten sie den Angestellten keine Informationen zur Verfügung. Weiterhin bestanden keine geeigneten Sicherheitsmaßnahmen gegen einen Zugriff Unbefugter.	Link	Link	
20.8.19	Datainspektionen	Schweden	20.000 €	200.000 SEK	Art. 5 I c, 9. 35, 36	Schule in Skellefteå	An der Schule war ein Pilotprojekt zur Überwachung der regelmäßigen Anwesenheit der Schüler durchgeführt worden: Mit Gesichts-Scans wurden die biometrischen Daten erhoben und für die Überprüfung der Anwesenheit ausgewertet. Nach Ansicht der Aufsichtsbehörde wurden damit Daten ohne rechtliche Grundlage verarbeitet, da die Schule zwar Einwilligungen eingeholt hatte, aufgrund des Ungleichgewichts zwischen Schülern und Schulverwaltung diese aber nicht wirksam sein konnten. Auch war die Behörde nicht vor dem Start des Projekts aufgrund des hohen Datenschutzrisikos konsultiert worden.	Link	Link	
2.7.19	ANSPDCP	Rumänien	15.000 €	71.028 RON	Art. 32	World Trade Center Bucharest SA	Daten von 46 Hotelgästen waren von Unbefugten abfotografiert und teils später online veröffentlicht worden. Die Daten waren auf einer Liste in Papierform beim Frühstücksbüffet zur Überprüfung der Gäste genutzt worden, aber nicht genügend vor einem Zugriff Dritter geschützt worden.	Link		
25.4.19	UODO	Polen	13.000 €	55.750, 50 PLN	Art. 5 I f, 32 I b	Dolnośląski Związek Piłki Nożnej (Niederschlesischer Fußballverband)	Der Fußballverband hatte versehentlich detaillierte Informationen zu Schiedsrichtern, denen eine Lizenz erteilt worden war, online auf seiner Webseite veröffentlicht. Erschwerend wirkte sich auf die Bußgeldhöhe aus, dass der Verstoß 3 Jahre andauerte und über 500 Schiedsrichter betroffen waren. Mildernd wurde die Kooperation mit der Aufsichtsbehörde berücksichtigt, sowie die Tatsache, dass den Betroffenen offenbar faktisch kein Schaden durch die Datenschutzverletzung entstanden war.	Link		
Jul 19	DSB	Österreich	11.000 €	(noch nicht final) (10.000 € + 1.000 € Verfahrenskosten)	Art. 6	Fußball-Trainer	Ein Trainer hatte mit einem Handy versteckt Aufnahmen von seinen Spielerinnen in der Umkleide und Dusche gemacht. Ein Strafverfahren diesbezüglich war eingestellt worden. Der Trainer hat gegen das Bußgeld Beschwerde eingelegt.	Link		

2019	Commissioner for Personal Data Protection	Zypern	10.000 €	-	Art. 5 I c, Art. 6	Zeitung	Eine Zeitung hatte die Namen und Gesichter zweier Polizisten veröffentlicht, die an einer (angeblich rechtswidrigen) Verhaftung beteiligt waren, sowie das Bild eines dritten Polizisten. Der Commissioner verhängte das Bußgeld, da bei der Abwägung zwischen dem Recht der Polizisten auf den Schutz ihrer Daten und dem Recht auf Information der Öffentlichkeit das Recht der Polizisten höher wiege. Schließlich hätte der Bericht nach Ansicht der Behörde auch mit Intialen und verpixelten Gesichtern dem Informationsbedürfnis der Öffentlichkeit genügt, ohne die Betroffenen zu identifizieren. Es lag mithin ein Verstoß gegen den Grundsatz der Datenminimierung vor.	Link		
21.3.19	UOOU	Tschechien	9.704 €	250.000 CZK	Art. 5 I c, e	unbekannt	Das Unternehmen hatte gegen den Grundsatz der Datenminimierung und der Speicherbegrenzung verstoßen, indem es zunächst mit aufgezeichneten Telefonaten zu viele Daten erhob und dann eine regelmäßige Speicherzeit von 10 Jahren vorsah. Die Aufsichtsbehörde verhängte zugleich Auflagen zur Abhilfe dieser Missstände, denen das Unternehmen nachkommen will.	Link		
17.4.19	NAIH	Ungarn	9.400 €	3.000.000 HUF	Art. 5 I a, 6	unbekannt	Der Verantwortliche hatte die Verarbeitung von personenbezogenen Daten nach Ansicht der Aufsichtsbehörde auf die falsche Rechtsgrundlage gestützt und damit gegen den Grundsatz der Transparenz verstoßen.	Link		
26.8.19	DSI	Lettland	7.000 €	-	Art. 17	Online-Händler	Ein Online-Händler hatte wiederholt einem ehemaligen Kunden, der um Löschung seiner Handynummer gebeten hatte, Werbe-SMS geschickt. Abgesehen davon, dass er die Anfrage des Kunden nicht beantwortete, arbeitete er auch mit der Aufsichtsbehörde nicht zusammen und kam deren Aufforderung zur Auskunft nicht nach, sodass das Bußgeld entsprechend höher ausfiel.	Link		
26.3.19	CPDP bzw. KZLD	Bulgarien	5.100 €	10.000 BGN	Art. 5 I a, 6	"A.R." EOOD	Das Unternehmen hatte die Daten des Betroffenen genutzt, um einen mit dem Betroffenen geschlossenen Arbeitsvertrag an die bulgarische Steuerbehörde zu melden, obwohl der Mann zum Zeitpunkt der Meldung inhaftiert war. Die Weitergabe der Daten geschah ohne dessen Wissen und Zustimmung.	Link		
2018	AEPD	Spanien	5.000 €	-	Art. 5 I d	Vodafone Espana	Vodafone Espana gab Daten eines Kunden an ein Bonitätsregister (BADEXCUG) weiter, obwohl bereits entschieden worden war, dass die Kosten dem Kunden zu erstatten seien. Damit kam das Unternehmen seiner Pflicht zur unverzüglichen Berichtigung nicht nach.	Link	Link	Link
18.2.19	IDPC	Malta	5.000 €	-	Art. 32	Lands Authority (Liegenschafts-behörde)	Die Daten auf der Webseite der LA (u.a. Ausweisdaten, E-Mail-Korrespondenz, Erklärungen zu Anträgen) waren durch einen Fehler im System auffind- und einsehbar. Die IDPC sperrte vorübergehend die Webseite und verhängte das Bußgeld wegen der unzureichenden Sicherheitsmaßnahmen.	Link	Link	
2019	Commissioner for Personal Data Protection	Zypern	5.000 €	-	Art. 15	Krankenhaus	Eine Patientin ersuchte um Auskünfte über die von ihr gespeicherten Daten bei dem Krankenhaus, dieses konnte allerdings ihre Akte nicht mehr auffinden. Das Bußgeld wurde erhoben, da bei der rechtmäßigen Datenverarbeitung auch die Sicherheit vor versehentlicher Zerstörung oder anderweitigem Verlust der Daten gewährleistet sein muss.	Link		
12.9.18	DSB	Österreich	4.800 € (nur 2.400 € nach DSGVO)		Art. 5 I a, c, 6 I	Wettlokal	Der Inhaber mehrerer Wettlokale hatte vor einem eine Überwachungskamera angebracht, deren Aufnahmebereich sich auch auf den öffentlichen Verkehrsbereich in einem Abstand bis 20m vor dem Lokal erstreckte. Auf die Überwachungskamera wurde nicht hingewiesen (Verstoß gegen österreichisches Recht, § 13 BSD). Da vorübergehende Passanten nicht mit Bildaufnahmen rechnen mussten und erst recht nicht mit deren Speicherung, wurde ein Bußgeld nach Landesrecht (ebenfalls 2.400 €) und eines nach DSGVO verhängt, da der Verstoß zum einen mehrere Monate andauerte und um den Betreiber des Wettlokals von weiteren Verstößen in seinen anderen Lokalen abzuschrecken.	Link		
4.3.19	NAIH	Ungarn	3.200 €	1.000.000 HUF	Art. 5 I b, c, 6, 13 III, 17 I	Finanzinstitution	Ein Kunde hatte die Berichtigung und Löschung seiner personenbezogenen Daten gefordert. Die Löschung seiner Telefonnummer war mit der Begründung abeglehnt worden, dass ein berechtigtes Interesse der Löschung entgegenstehe, da die Institution eine Forderung gegen den Kunden durchsetzen wolle. Die Aufsichtsbehörde verneinte das berechtigte Interesse bzgl. der Telefonnummer, da die Postadresse zur Kommunikation ausreiche und sonst ein Verstoß gegen den Grundsatz der Datenminimierung vorliege.	Link		
28.2.19	NAIH	Ungarn	3.200 €	1.000.000 HUF	Art. 5 I a, 6	Bürgermeister von Kecskemét	Das Bürgermeisteramt hatte gegenüber einer von ihm beaufsichtigten Organisation die personenbezogenen Daten eines Whistleblowers rechtswidrig offengelegt. Der Angestellte hatte eine Beschwerde über seinen Arbeitgeber beim Bürgermeisteramt eingelegt. Daraufhin hatte das Amt die Einrichtung über das Vorliegen der Beschwerde unterrichtet und Ermittlungen eingeleitet. Als die Organisation die Offenlegung des Beschwerdeinhalts forderte, wurde versehentlich auch der Name des Beschwerdeführers weitergegeben. Die Aufsichtsbehörde berücksichtigte erschwerend die Folgen für den Betroffenen: Dieser war nach der Offenlegung seines Namens entlassen worden.	Link		
18.12.18	NAIH	Ungarn	3.200 €	1.000.000 HUF	Art. 12 IV, 13, 15, 18 I c	unbekannt	Einem Betroffenen wurden bzgl. Videoüberwachung bei Auskunftsersuchen weder die Aufnahmen noch Informationen über deren Speicherung und weitere Verwendung oder bestehendes Beschwerderecht zur Verfügung gestellt.	Link		
13.5.19	UOOU	Tschechien	3.105 €	80.000 CZK	Art. 5 I a, b, 32 I	unbekannt	Die Daten des Betroffenen waren zur Führung eines Girokontos bei dem Unternehmen gespeichert. Als der Betroffene ein Jahr nach Eröffnung des Kontos kontaktiert wurde und sich herausstellte, das jemand anders das Konto unter seinem Namen eröffnet hatte, wurde es auf Ersuchen des Betroffenen geschlossen. Allerdings waren nach Ansicht der Aufsichtsbehörde die internen Kontrollmechanismen des Unternehmens, die technischen und organisatorischen Maßnahmen ungenügend, da erst ein Jahr nach Vertragsschluss durch Kontakt mit dem Betroffenen der rechtswidrige Vertragsschluss dem Unternehmen bekannt wurde.	Link		
5.7.19	ANSPDCP	Rumänien	3.000 €	14.173,50 RON	Art. 32	Legal Company & Tax Hub SRL	Aufgrund ungenügender Sicherheitsmaßnahmen auf der Webseite waren fast zwei Monate lang personenbezogene Daten wie Adressen, Beruf, Transaktionsdetails für Unbefugte zugänglich.	Link	Link	
Jul 19	ANSPDCP	Rumänien	2.500 €	11.834,25 BGN	Art. 5 I c, 6, 12, 13	Uttis Industries SRL	Ob den Informationspflichten u.a. über die Verwendung seines Videoüberwachungssystems von dem Unternehmen nachgekommen wurde, konnte dieses nicht ausreichend nachweisen.	Link		
20.12.18	DSB	Österreich	2.200 €	(1.000 € nach DSGVO, Rest nach Österreichischem DSG)	Art. 5 I a, c, 6	Privatperson	Ein Mann hatte private Gemeinschaftsbereiche in einer Wohnanlage videoüberwacht, die nicht allein zu seinem Wohnbereich gehörten (u.a. Garten, Parkplatz, Zugangsbereiche). Auf die Videoüberwachung wurde nach österreichischem Recht auch nicht hinreichend hingewiesen.	Link		
28.5.19	APD	Belgien	2.000 €	-	Art. 5 I b, 6	Bürgermeister	Ein Bürgermeister hatte Kontakt mit den Beschwerdeführern über ihren Architekten wegen einer baulichen Änderungsmaßnahme. Der Bürgermeister nutzte bei den darauffolgenden Kommunalwahlen dann die dadurch erhaltenen E-Mail-Adressen für die Zusendung von Wahlwerbung.	Link		
5.4.19	NAIH	Ungarn	1.900 €	600.000 HUF	Art. 15	Arbeitgeber	Dem wiederholten Auskunftsersuchen eines Angestellten wurde nicht nachgekommen.	Link		
2018	DSB	Österreich	1.800 €	-	unbekannt	Kebab Restaurant	Datenschutzrechtswidrige Nutzung einer Videoüberwachungsanlage	Link		
20.2.19	NAIH	Ungarn	1.560 €	500.000 HUF	Art. 5 I a, c	Schuldeneintreiber	Der Antrag eines Betroffenen auf Auskunft und Löschung seiner personenbezogenen Daten führte dazu, dass der Verantwortliche zunächst weitere persönliche Daten erhob, um ihn identifizieren zu können. Dann lehnte er aber das Löschbegehren ab aufgrund der Aufbewahrungsfristen für die Rechnungslegung und interner Vorschriften, informierte hierüber allerdings nicht ordnungsgemäß.	Link		
8.2.19	NAIH	Ungarn	1.560 €	500.000 HUF	Art. 5 I d	Bank	Die Bank war dem Ersuchen des Betroffenen um Berichtigung einer vorliegenden falschen Telefonnummer nicht nachgekommen. Als Folge dessen versendete die Bank wiederholt Informationen über die Kreditschulden des Betroffenen als SMS an die falsche Nummer.	Link		
4.2.19	UOOU	Tschechien	1.168 €	30.000 CZK	Art. 5 I a, 13	Autovermietung	Ein Kunde der Autovermietung stellte fest, dass die GPS-Daten seiner Fahrt erhoben wurden und legte Beschwerde ein. Der Autovermieter verwies auf den Schutz seines Interesses daran zu wissen, wo sich sein Auto befindet (für den Fall eines Diebstahls oder Unfalls), als legitimen Zweck zur Erhebung nach Art. 6 I f DSGVO. Die Aufsichtsbehörde verneinte die Abwägung der Interessen zugunsten des Unternehmens, sodass kein legitimer Zweck gegeben sei. Zudem war weder in den AGB noch im Vertrag auf das GPS-Tracking hingewiesen worden, wodurch die Informationspflicht verletzt wurde.	Link		
4.2.19	UOOU	Tschechien	1.168 €	30.000 CZK	Art. 5 I f	Kreditvermittlung	Das Unternehmen hatte die Daten von ca. 300 Kunden (u.a. Sozialversicherungsnummern und Telefonnummern) in Verbraucherkreditanträgen etwa zwei Wochen frei in einem Karton in der Garage eines Mehrfamilienhauses gelagert, dieser wurde dann später neben einem Müllcontainer gefunden. Die Aufbewahrung verstieß damit gegen das Prinzip, dass Daten sicher vor Beeinträchtigung, Zugriff und Zerstörung verarbeitet und gespeichert werden müssen (Integrität und Vertraulichkeit).	Link		

Aug 19	Landesgericht Feldkirch	Österreich	800 €	(kein Bußgeld, sondern vom Gericht zuerkannter Schadenersatz)		Post	Ein Vorarlberger Anwalt verklagte die Österreichische Post auf immateriellen Schadenersatz. Er war einer der Betroffenen, deren Parteiaffinität von der Post zusätzlich zur Adresse gespeichert wurde. Nach Ansicht des Gerichts handelt es sich bei der politischen Zugehörigkeit um besonders sensible Daten, die nicht ohne Einwilligung und Wissen des Betroffenen erhoben werden durften, weshalb ihm immaterieller Schadensersatz zugesprochen wurde. Die Post hatte die Parteiaffinitäten von über 2 Mio. Österreichern erhoben und diese Informationen an Parteien verkauft. In dem verhandelten Fall konnte nach Ansicht des Gerichts die Weitergabe der Daten nicht festgestellt werden, sonst wäre der Schadenersatz höher ausgefallen. Das Urteil ist noch nicht rechtskräftig. Die Post geht noch dagegen vor, da sie sonst von den anderen Betroffenen evtl. höhere Schadenersatzklagen zu fürchten hat.	Link	
26.2.19	UOOU	Tschechien	773 €	20.000 CZK	Art. 15	Unternehmen	Das Unternehmen hatte den Betroffenen mit Angeboten zum Aktienhandel kontaktiert und keine Auskunft innerhalb der gesetzlichen Frist erteilt, als dieser mehrfach nachfragte, wie das Unternehmen an seine Kontaktdaten gekommen war. Die Aufsichtsbehörde wurde aufgrund der Beschwerde des Betroffenen tätig.	Link	
28.2.19	UOOU	Tschechien	580 €	15.000 CZK	Art. 5 I f	Online-Rollenspiel-Plattform	Der Betreiber eines Online-Rollenspiels hatte ein Datenleck für etwa 30 Minuten aufgrund mangelnder Sicherheitsvorkehrungen zu vermelden. In diesem Zeitfenster konnten Unbefugte auf Daten der Spieler zugreifen (E-Mailadresse, Spielerkonto-Passwort und IP-Adresse). Der Betreiber wies die Schuld von sich und gab dem Programmierer die Schuld, seine Macht missbraucht haben, um auf die Daten zuzugreifen. Da außerdem nur kurzzeitig und nur relativ „unwichtige" personenbezogene Daten von einer begrenzten Anzahl Personen betroffen waren, fiel das Bußgeld vergleichsweise gering aus. Der Verantwortliche führte zum Beispiel auch aus, dass die Anzahl der Spielerkonten nicht auf eine ebenso große Anzahl betroffener natürlicher Personen schließen lasse, da es üblich sei, dass Spieler, um sich Vorteile im Spiel zu verschaffen, (entgegen der Nutzungsbedingungen) mehrere Spielerkonten eröffneten.	Link	
4.12.18	CPDP bzw. KZLD	Bulgarien	511 €	1.000 BGN	Art. 5 I b	"T.B.A.B." EAD (Bank)	Ein früherer Kunde der Bank wurde angerufen, um Informationen über einen Nachbarn, der dort Kunde war, einzuholen. Der ehemalige Kunde schrieb die Bank an, seine Daten zu löschen, da das Vertragsverhältnis 2015 geendet hatte. Er erhielt jedoch keine Antwort und es erfolgte ein weiterer Anruf bzgl. eines Dritten. Daraufhin legte der Mann Beschwerde bei der CPDP ein. Diese erhob das Bußgeld wegen des fehlenden legitimen Zwecks für die Datenverarbeitung, da der Sachverhalt jedoch nicht vollständig nachgewiesen werden konnte und die Bank sich kooperativ verhielt und den Anruf einem eigenmächtig handelnden Angestellten zuschrieb, blieb es bei einem geringen Betrag verbunden mit der Auflage, die Daten des ehemaligen Kunden endgültig zu löschen.	Link	Link
8.4.19	CPDP	Bulgarien	511 €	1.000 BGN	Art. 5 I a, 6, 9 I, II	Arztpraxis	Ein Patient stellte fest, dass er bei einem Arzt als Patient geführt wurde, bei dem er nie gewesen war, und dass er deswegen im Register der Krankenkasse bei verschiedenen Hausärzten gemeldet war. Seine Daten waren irrtümlich durch eine Software übertragen worden beim Verkauf der Praxis seines früheren Hausarztes: In der Software war eine Löschung der Patienten nicht vorgesehen, nur ein Wechsel zwischen aktiv und inaktiv im Status. Der Beschwerdeführer war bereits inaktiv gesetzt vor der Aufgabe der Arztpraxis. Bei der Übernahme der Praxis hatte der neue Arzt auch die Software übernommen, der Betroffene war aber versehentlich wieder als aktiv geführt. Es wurde eine Löschung der Patientendaten aus dem System des Arztes angeordnet und ein Bußgeld wurde verhängt, da es sich bei Gesundheitsdaten um besonders sensible Daten nach Art. 9 DSGVO handelt.	Link	Link
22.2.19	CPDP bzw. KZLD	Bulgarien	511 €	1.000 BGN	Art. 5 I b, c, 12, 15 I a-c, g, III	Arbeitgeber	Ein Mitarbeiter verlangte von seinem Arbeitgeber Auskunft über seine personenbezogenen Daten und seine Nachfrage wurde nicht rechtzeitig und nicht vollständig beantwortet.	Link	
17.1.19	CPDP bzw. KZLD	Bulgarien	511 €	1.000 BGN	Art. 5 I a, 6	Bank	Die Bank hatte die personenbezogenen Daten eines Studenten ohne Rechtsgrundlage erhalten.	Link	
25.10.18	UOOU	Tschechien	386 €	10.000 CZK	Art. 15	Unternehmen	Der Verantwortliche hatte auf Anfrage zwar die Daten des Betroffenen von seiner Website gelöscht, allerdings keine Auskunft über die erhobenen und gespeicherten Daten erteilt, auch nach mehrfacher Aufforderung.		
10.1.19	UOOU	Tschechien	386 €	10.000 CZK	Art. 6 I	Arbeitgeber	Ein Arbeitgeber hatte auf seiner Facebookseite personenbezogene Daten eines früheren Angestellten trotz Aufforderung nicht gelöscht.	Link	
2018	DSB	Österreich	300 €	-	unbekannt	Kfz-Halter	Datenschutzrechtswidrige Nutzung einer Dashcam	Link	
06.05.19	UOOU	Tschechien	193 €	5.000 CZK	Art. 15	Unternehmen	Das Verfahren wegen eines Verstoßes gegen Art. 5 DSGVO wurde eingestellt, aber ein Bußgeld wegen Verstoßes gegen die Auskunftspflicht verhängt.	Link	
2019	DSB	Österreich				Spotify	Die Datenschutzorganisation noyb (none of your business) hat Tests durchgeführt, wie das Unternehmen mit Auskunftsanfragen nach DSGVO umgeht. Da Spotify nur unvollständige Informationen z.B. über die Weitergabe von Daten bereitstellte, hat noyb im Namen der Nutzer Beschwerde bei der österreichischen DSB eingereicht. Die DSB solle die weiteren Schritte ergreifen, d.h. die Beschwerden an die Aufsichtsbehörde des Hauptsitzes des Unternehmens in der EU weiterleiten und mit dieser Behörde zusammenarbeiten.	Link	
2019	DSB	Österreich				Amazon Prime	Die Datenschutzorganisation noyb (none of your business) hat Tests durchgeführt, wie das Unternehmen mit Auskunftsanfragen nach DSGVO umgeht. Da Amazon Prime nur mit der Herausgabe unvollständiger Rohdaten und nur teilweise verständlich darauf reagierte, hat noyb im Namen der Nutzer Beschwerde bei der österreichischen DSB eingereicht. Die DSB solle die weiteren Schritte ergreifen, d.h. die Beschwerden an die Aufsichtsbehörde des Hauptsitzes des Unternehmens in der EU weiterleiten und mit dieser Behörde zusammenarbeiten.	Link	
2019	DSB	Österreich				Apple Music	Die Datenschutzorganisation noyb (none of your business) hat Tests durchgeführt, wie das Unternehmen mit Auskunftsanfragen nach DSGVO umgeht. Da AppleMusic nur mit der Herausgabe unvollständiger Rohdaten und nur teilweise verständlich darauf reagierte, hat noyb im Namen der Nutzer Beschwerde bei der österreichischen DSB eingereicht. Die DSB solle die weiteren Schritte ergreifen, d.h. die Beschwerden an die Aufsichtsbehörde des Hauptsitzes des Unternehmens in der EU weiterleiten und mit dieser Behörde zusammenarbeiten.	Link	
2019	DSB	Österreich				Dazn	Die Datenschutzorganisation noyb (none of your business) hat Tests durchgeführt, wie das Unternehmen mit Auskunftsanfragen nach DSGVO umgeht. Da Dazn die Anfragen komplett ignorierte, hat noyb im Namen der Nutzer Beschwerde bei der österreichischen DSB eingereicht. Die DSB solle die weiteren Schritte ergreifen, d.h. die Beschwerden an die Aufsichtsbehörde des Hauptsitzes des Unternehmens in der EU weiterleiten und mit dieser Behörde zusammenarbeiten.	Link	
2019	DSB	Österreich				Filmmit	Die Datenschutzorganisation noyb (none of your business) hat Tests durchgeführt, wie das Unternehmen mit Auskunftsanfragen nach DSGVO umgeht. Da Filmmit zwar manuell auf Anfragen reagierte, aber detaillierte Informationen zu den Empfängern der verarbeiteten Daten schuldig blieb, hat noyb im Namen der Nutzer Beschwerde bei der österreichischen DSB eingereicht. Die DSB solle die weiteren Schritte ergreifen, d.h. die Beschwerden an die Aufsichtsbehörde des Hauptsitzes des Unternehmens in der EU weiterleiten und mit dieser Behörde zusammenarbeiten.	Link	
2019	DSB	Österreich				Netflix	Die Datenschutzorganisation noyb (none of your business) hat Tests durchgeführt, wie das Unternehmen mit Auskunftsanfragen nach DSGVO umgeht. Da Netflix zwar verständlich antwortete, aber nur unvollständige Informationen z.B. über die Weitergabe von Daten bereitstellte, hat noyb im Namen der Nutzer Beschwerde bei der österreichischen DSB eingereicht. Die DSB solle die weiteren Schritte ergreifen, d.h. die Beschwerden an die Aufsichtsbehörde des Hauptsitzes des Unternehmens in der EU weiterleiten und mit dieser Behörde zusammenarbeiten.	Link	
2019	DSB	Österreich				SoundCloud	Die Datenschutzorganisation noyb (none of your business) hat Tests durchgeführt, wie das Unternehmen mit Auskunftsanfragen nach DSGVO umgeht. Da SoundCloud die Anfragen komplett ignorierte, hat noyb im Namen der Nutzer Beschwerde bei der österreichischen DSB eingereicht. Die DSB solle die weiteren Schritte ergreifen, d.h. die Beschwerden an die Aufsichtsbehörde des Hauptsitzes des Unternehmens in der EU weiterleiten und mit dieser Behörde zusammenarbeiten.	Link	
2019	DSB	Österreich				Youtube	Die Datenschutzorganisation noyb (none of your business) hat Tests durchgeführt, wie das Unternehmen mit Auskunftsanfragen nach DSGVO umgeht. Da Youtube nur unvollständige Informationen z.B. über die Weitergabe von Daten bereitstellte, hat noyb im Namen der Nutzer Beschwerde bei der österreichischen DSB eingereicht. Die DSB solle die weiteren Schritte ergreifen, d.h. die Beschwerden an die Aufsichtsbehörde des Hauptsitzes des Unternehmens in der EU weiterleiten und mit dieser Behörde zusammenarbeiten.	Link	

2019	DPC	Irland			Facebook	Derzeit sind bei der Aufsichtsbehörde Irlands, wo sich die Hauptniederlassung Facebooks in der EU befindet, mehrere Untersuchungen wegen Verstößen gegen das Transparenzgebot und die faire Verarbeitung, nach Treu und Glauben, im Gange.	Link	Link (S.50f)
2019	DPC	Irland			WhatsApp	Derzeit sind bei der Aufsichtsbehörde Irlands, wo sich die Hauptniederlassung WhatsApps in der EU befindet, Untersuchungen wegen Verstößen gegen das Transparenzgebot und die faire Verarbeitung, nach Treu und Glauben, im Gange.	Link	Link (S.50f)
2019	DPC	Irland			Apple	Derzeit sind bei der Aufsichtsbehörde Irlands, wo sich die Hauptniederlassung Apples in der EU befindet, Untersuchungen wegen Verstößen gegen das Transparenzgebot und die faire Verarbeitung, nach Treu und Glauben, im Gange.	Link	Link (S.50f)
2019	DPC	Irland			Twitter	Derzeit sind bei der Aufsichtsbehörde Irlands, wo sich die Hauptniederlassung Twitters in der EU befindet, Untersuchungen wegen Verstößen gegen die DSGVO durch unzureichende technische und organisatorische Maßnahmen zum Datenschutz im Gange. Es gingen 2018 zahlreiche Beschwerden ein, dass Datenlecks bei Twitter bestünden.	Link	Link (S.50f)
2019	DPC	Irland			LinkedIn	Derzeit ist bei der Aufsichtsbehörde Irlands, wo sich die Hauptniederlassung LinkedIns in der EU befindet, eine Untersuchung wegen Verstößen gegen die faire Verarbeitung, nach Treu und Glauben, im Gange.	Link	Link (S.50f)
2019	DPC	Irland			Instagram	Derzeit ist bei der Aufsichtsbehörde Irlands, wo sich die Hauptniederlassung in der EU befindet, eine Untersuchung gegen Instagram wegen Verstößen die faire Verarbeitung, nach Treu und Glauben, im Gange.	Link	Link (S.50f)
12.2.19	DSB	Österreich	Unterlassungsanordnung		Post	Die Post hatte zusätzlich zu den Namen und Adressen mutmaßliche Parteiaffinitäten von ca. 2,2 Mio. Österreichern erhoben und gespeichert sowie diese Informationen jahrelang an Parteien verkauft. Die Österreichische Datenschutzaufsichtsbehörde hatte diesbezüglich ein Prüfungsverfahren eingeleitet und festgestellt, dass die Post die Parteineigung nicht statistisch erheben und speichern, erst recht nicht damit handeln darf, sofern nicht im Einzelfall eine Einwilligung oder ein anderer gesetzlicher Grund vorliegt. Die Post wurde angewiesen, diese Praxis künftig zu unterlassen und alle diesbezüglich widerrechtlich gespeicherten Daten zu löschen. Weiterhin bemängelte die DSB die Datenschutzfolgenabschätzung der Post und wies sie an, diese zu wiederholen. Die Post geht derzeit gegen die Anordnung vor, da sie die Meinung vertritt, legal gehandelt zu haben.	Link	Link
Aug 19	EDÖB	Schweiz	-		CSS (Krankenkasse)	Die Krankenkasse CSS hatte in ihrem Online-Portal Rechnungen an die falschen Kunden versendet, dies machte nach Hochrechnung der CSS etwa 0,07 % aller Rechnungen aus, was bei den verarbeiteten 17 Mio. Rechnungen im Jahr aber immerhin noch fast 12.000 falsch versendete Rechnungen bedeutete. Da es sich bei Gesundheitsdaten um besonders sensible und schützenswerte Daten handelt, hat die CSS das System überarbeitet, sodass keine Rückschlüsse auf die betroffene Person mehr möglich sein sollen, sollte eine Rechnung an den falschen Empfänger gehen. Der Eidgenössische Datenschutzbeauftragte sah daraufhin keinen weiteren Handlungsbedarf.	Link	
Mai 18 – Aug 19		USA			Twitter	Twitter hat offenbar über ein Jahr lang versehentlich Nutzerdaten an Werbekunden weitergegeben. Passwörter waren nicht betroffen. Nach einer Stellungnahme des Unternehmens wurde das Problem am 5.8.19 behoben. Welche Konsequenzen Twitter für diese Datenpanne drohen, steht noch nicht fest.	Link	Link
Aug 19		USA			Entertainment Software Association (Veranstalter der E3)	Auf der Website der Spielemesse E3 waren einige Tage lang die Daten von 2025 Fachbesuchern einsehbar. Obwohl die Liste dort gelöscht wurde, ist sie wohl von anderen kopiert worden und noch immer auffindbar. Welche Konsequenzen für diese Datenpanne drohen, steht noch nicht fest.	Link	
Jul 19		USA/Kanada			Capital One	Durch einen Hackerangriff wurden über 100 Mio. Kundendaten (u.a. Adressen, Kreditkarteninformationen) von US-Kunden und 6 Mio. Daten von kanadischen Kunden der Bank erbeutet. Eine falsch konfigurierte Firewall soll den Datendiebstahl ermöglicht haben. Derzeit wird noch gemutmaßt, ob evtl. auch die europäische Partnerbank Unicredit betroffen gewesen sein könnte. Eine Klage gegen die Täterin ist in Washington anhängig, welche Folgen sich für Capital One ergeben, steht noch nicht fest.	Link	Link
Aug 19		Korea/ International			Suprema	Auf der Plattform Biostar 2 des koreanischen Unternehmens Suprema waren über 1 Mio. biometrische Daten (z.B. Fingerabdrücke) für etwa eine Woche (nach Entdeckung des Lecks durch Datenschützer) öffentlich zugänglich. Die Software wird von vielen Unternehmen international zur Zugangskontrolle und z.B. auch von der britischen Polizei eingesetzt. Welche Konsequenz das immense Datenleck haben wird, ist noch unklar.	Link	Link Link
2017-2019		USA/ International			Apple	Bis zum 7.2.19, als Google-Forscher Apple verständigten und das Unternehmen die Sicherheitslücke schloss, sollen Nutzer von I-Phones ausspioniert worden sein. Die Malware soll durch den Besuch von ungenannten Websites übertragen worden sein. Das Ausmaß der Folgen der Sicherheitslücke ist noch nicht umfassend bekannt, aber möglicherweise waren chinesische Dissidenten Ziel des Angriffs. Was die Konsequenzen des Vorfalls sein werden, ist noch unklar.	Link	Link
Sep 19		USA/ International			Facebook	Rund 420 Mio. Telefonnummern von Facebook-Nutzern wurden online veröffentlicht. Dabei handele es sich aber um alte Daten, da die aufgetauchte Liste mit Hilfe einer inzwischen abgeschalteten Funktion, Freunde auf Facebook mittels ihrer Telefonnummer zu finden, erstellt worden sei. Was das Ziel der Veröffentlichung oder auch der Erstellung der Liste war, ist unbekannt. Ebenso ist unklar, mit welchen Konsequenzen Facebook für den neuen Datenschutzskandal rechnen muss.	Link	
13.8.18	UODO	Polen	gestartete Überprüfung			Das Erstellen einer "schwarzen Liste" unzuverlässiger Patienten ruft Bedenken der Datenschutzbehörde hervor. Sie prüft von Amts wegen, ob dies mit der DS-GVO vereinbar ist.	Link	
9.7.19	Belgian Data Protection Authority (DPA)	Belgien	Rüge (reprimand)		FPS Public Health	FPS Public Health wurde gerügt, weil es nicht auf die Ausübung des Auskunftsrechts eines Bürgers reagierte.	Link	Link
15.1.19	DSB	Österreich	Bescheid, Beschwerde	Art. 12 IV, 17 DS-GVO	Arztsuch-/ Bewertungsportal	Der Beschwerdeführer ist Arzt, die Beschwerdegegnerin betreibt ein Arztsuch-/Bewertungsportal im Internet. Dort wurden Berufsadresse, Telefonnummer, Öffnungszeiten, Diplome, Zertifikate und Name des Beschwerdeführers als Arztprofils publiziert. Patienten können auf dem Portal Arztbesuche bewerten und ihre Erfahrungen schildern. Die Datenschutzbehörde kam zu dem Ergebnis, schlussendlich eine Verletzung des Rechts auf Geheimhaltung zu verneinen ist. Die berechtigten Interessen der das Portal nutzenden Patienten überwiegen die des Arztes. Daher ist Art. 17 I d DS-GVO nicht erfüllt, die Verarbeitung der personenbezogenen Daten ist rechtmäßig. Darüber hinaus ist sie nach Art. 17 III a DS-GVO zur Ausübung des Rechts auf freie Meinungsäußerung und Information erforderlich. Das Portal hat das Arztprofil zurecht nicht gelöscht.	Link	
16.11.18	DSB	Österreich	Bescheid, amtswegiges Prüfverfahren	Art. 6, 7 IV, 9, 12, 13, 14, 35, 37 DS-GVO	Allergie-Tagesklinik D*** GmbH	Die Verantwortliche ist eine GmbH mit Sitz in D***. Ihr Geschäftszweck ist die Diagnostik und Therapie von allergischen Erkrankungen mit Fokus auf Kinder und Familien. Angestellt waren drei Mitarbeiter im Management, 17 Ärzte, zwölf Büro-/Labormitarbeiter und zwei Ernährungsberater. Gesundheitsdaten als eine besondere Kategorie von Daten (vgl. Art. 9 DS-GVO wurden regelmäßig und umfassend verarbeitet. Die Datenschutzbehörde stellt einen Verstoß gegen die Pflicht zur Bestellung eines Datenschutzbeauftragten fest, bemängelte die Verpflichtung von Patienten zu unklaren, gesetzwidrigen Einwilligungen und rügte die Nichteinhaltung der Informationspflichten. Zudem wurde unzutreffenderweise davon ausgegangen, dass eine Datenschutz-Folgenabschätzung entbehrlich sei. Der Verantwortlichen wurde aufgetragen, innerhalb einer Frist von acht Wochen bei sonstiger Exekution die Mängel zu beheben (bzw. damit zu beginnen).	Link	
8.8.18	DSB	Österreich	Bescheid, amtswegiges Prüfverfahren	Art. 33, 34 DS-GVO	N*** Hilfs- und Rettungsverband, Landesverband ****	Am 12.11.2018 wurde eine Sicherheitsverletzung nach Art. 33 DS-GVO gemeldet, weil am 10.11.2018 ein Suchtgiftbuch verloren ging. Die Datenschutzbehörde trug dem Verantwortlichen auf, innerhalb von vier Wochen alle Personen, deren Gesundheitsdaten betroffen sind, zu informieren und dies nachzuweisen.	Link	
6.6.18	DSB	Österreich	Bescheid, Beschwerde	Art. 15 DS-GVO	Magistrat der Stadt Wien – MA 63 (Krankenhaus **** Wien)	Die Datenschutzbehörde entschied über die Datenschutzbeschwerde von Frau Nora A*** gegen den Magistrat der Stadt Wien – MA 63 (Krankenhaus **** Wien) wegen einer Verletzung im Recht auf Auskunft (unvollständig erteilter Auskunft). Der Beschwerde wurde stattgegeben, weil nicht darüber informiert wurde, wer konkret auf die Krankenakte zugegriffen hat. Der Beschwerdegegner wurde angewiesen, innerhalb von zwei Wochen die entsprechende Auskunft zu erteilen.	Link	