

## SEZNAM POUŽITÉ LITERATURY A ZDROJŮ

### Právní předpisy

- nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012
- nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
- směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES
- směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV
- směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii
- směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace
- směrnice Evropského parlamentu a Rady (EU) 2020/1828 ze dne 25. listopadu 2020 o zastupných žalobách na ochranu kolektivních zájmů spotřebitelů a zrušení směrnice 2009/22/ES
- zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)
- zákon č. 128/2000 Sb., o obcích (obecní zřízení)
- zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
- zákon č. 256/2004 Sb., o podnikání na kapitálovém trhu
- zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)
- zákon č. 500/2004 Sb., správní řád
- zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)
- zákon č. 262/2006 Sb., zákoník práce
- zákon č. 40/2009 Sb., trestní zákoník
- zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim
- zákon č. 89/2012 Sb., občanský zákoník
- zákon č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích)



- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- zákon č. 134/2016 Sb., o zadávání veřejných zakázek
- zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich
- zákon č. 257/2016 Sb., o spotřebitelském úvěru
- zákon č. 370/2017 Sb., o platebním styku
- zákon č. 170/2018 Sb., o distribuci pojištění a zajištění
- zákon č. 110/2019 Sb., o zpracování osobních údajů
- vyhláška č. 163/2014 Sb., o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry
- vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
- vyhláška č. 361/2016 Sb., o zabezpečení jaderného zařízení a jaderného materiálu
- vyhláška č. 7/2018 Sb., o některých podmínkách výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz a vydavatele elektronických peněz malého rozsahu
- vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
- vyhláška č. 141/2018 Sb., o hlášení závažných bezpečnostních a provozních incidentů osobami oprávněnými poskytovat platební služby
- vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu

## Literatura

- BĚLINA, M.; DRÁPAL, L. a kol. *Zákoník práce. Komentář*. 3. vyd. Praha: C. H. Beck, 2019.
- BERAN, J.; NÝDRLE, T.; STRNADEL, D. *Zákon o platebním styku. Komentář*. Praha: Wolters Kluwer, 2020.
- ČASTORÁL, Z. *Management rizik v současných podmínkách*. Praha: Univerzita Jana Amose Komenského, 2017.
- HURYCHOVÁ, K.; SÝKORA, M. *Compliance programy (nejen) v České republice*. Praha: Wolters Kluwer ČR, 2018.
- JIRÁSEK, P.; NOVÁK, L.; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti* [online]. Praha: Policejní akademie ČR v Praze: Česká pobočka AFCEA, 2013. ISBN 978-80-7251-397-0. Dostupné z: [https://afcea.cz/wp-content/uploads/2015/03/Slovník\\_Final\\_screen\\_v2\\_0.pdf](https://afcea.cz/wp-content/uploads/2015/03/Slovník_Final_screen_v2_0.pdf).
- LUKÁŠ, L. a kol. *Teorie bezpečnosti*. Zlín: Radim Bačuvčík – VeRBuM. 2017, 220 s. ISBN 978-80-87500-89-7.
- MAISNER, M.; VLACHOVÁ, B. *Zákon o kybernetické bezpečnosti (č. 181/2014). Komentář*. Praha: Wolters Kluwer, 2015.
- NONNEMANN, F. Soukromí na pracovišti. *Právní rozhledy*, 2015, č. 7.
- NONNEMANN, F. Trestní odpovědnost právnické osoby za neoprávněné nakládání s osobními údaji. *Právní rozhledy*, 2016, č. 20.



- NULÍČEK, M.; DONÁT, J.; NONNEMANN, F.; LICHOVNSKÝ, B.; TOMÍŠEK, J.; KOVAŘÍKOVÁ, K. *GDPR / Obecné nařízení o ochraně osobních údajů (2016/679/EU). Praktický komentář*. 2. aktualizované vydání. Praha: Wolters Kluwer, 2018.
- NULÍČEK, M.; DONÁT, J.; NONNEMANN, F.; LICHOVNSKÝ, B.; HABARTA, P.; KOVAŘÍKOVÁ, K. *Zákon o zpracování osobních údajů (110/2019 Sb.). Praktický komentář*. Praha: Wolters Kluwer, 2019.
- PATTYNOVÁ, J.; SUCHÁNKOVÁ, L.; ČERNÝ, J.; RŮŽIČKA, M. a kol. *Obecné nařízení o ochraně osobních údajů (GDPR). Zákon o zpracování osobních údajů. Komentář*. 2. vyd. Praha: Leges, 2019.
- SCHENKOVÁ, K.; LASÁK, J. a kol. *Compliance v podnikové praxi*. Praha: C. H. Beck, 2017.
- ŠÁMAL, P.; DĚDIČ, J.; GŘIVNA, T.; PÚRY, F.; ŘÍHA, J. *Trestní odpovědnost právnických osob. Komentář*. 2. vyd. Praha: C. H. Beck, 2018.
- VLACHOVÁ, B. *Zákon o elektronických komunikacích. Komentář*. Praha: C. H. Beck, 2017.
- ZUZÁK, R.; KÖNIGOVÁ, M. *Krizové řízení podniku*. 2. aktualizované a rozšířené vydání. Praha: Grada Publishing, a.s., 2009.

## Ostatní zdroje

- Aktuální instrukce a kontaktní údaje pro hlášení porušení zabezpečení osobních údajů, dostupné z: <https://www.uoou.cz/poruseni-zabezpeceni/ds-5020/archiv=1>.
- Databáze registrovaných subjektů je dostupná z: <https://www.ctu.cz/vyhledavaci-databaze/evidence-podnikatelu-v-elektronickych-komunikacich-podle-vseobecneho-opraveni-od-2022>.
- Data Breach Investigations Report 2022 připravený americkou telekomunikační společností Verizon. Dostupné z: <https://www.verzion.com/business/resources/reports/dbir/>.
- ENISA. Reference Incident Classification Taxanomy. Dostupné z: <https://www.enisa.europa.eu/publications/reference-incident-classification-taxanomy/>.
- Formulář při hlášení incidentu českému ÚOOÚ. Dostupný z: [https://www.uoou.cz/assets/File.ashx?id\\_org=200144id\\_dokumenty=46004](https://www.uoou.cz/assets/File.ashx?id_org=200144id_dokumenty=46004).
- Guidelines 01/2021 on Examples regarding Data Breach Notification, dostupná z: [https://edpb.europa.eu/sites/default/files/consultation/edpb\\_guidelines\\_202101\\_databreachnotificationexamples\\_v1\\_en.pdf](https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf).
- Guidelines for identifying a controller or processor's lead supervisory authority, 16/ENWP 244, dostupné z: [https://ec.europa.eu/information\\_society/newsroom/image/document/2016-51/wp244\\_en\\_40857.pdf](https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf).
- Metodika hlášení kybernetického incidentu NÚKIB dostupná z: [https://www.nukib.cz/download/publikace/podpurne\\_materialy/2022-02-21\\_Metodika-hlaseni-incidentu\\_1.0.pdf](https://www.nukib.cz/download/publikace/podpurne_materialy/2022-02-21_Metodika-hlaseni-incidentu_1.0.pdf).
- Metodické pokyny pro hodnocení a způsob informování o závažném narušení bezpečnosti a ztrátě integrity sítí a služeb elektronických komunikací, dostupných z: <https://www.ctu.cz/sites/default/files/obsah/ctu-new/formulare/oznamovaci-povinnost-a-evidence/metodicke-pokyny-k-zavaznemu-naruseni.docx>.
- Metodický pokyn Ministerstva zdravotnictví poskytovatelům zdravotních služeb ke kybernetické bezpečnosti. Dostupné z: [https://ncez.mzcr.cz/sites/default/files/Attachment/Metodika-indetifikace\\_a\\_spr%C3%A1vy\\_informa%C4%8Dn%C3%ADch\\_aktiv.docx](https://ncez.mzcr.cz/sites/default/files/Attachment/Metodika-indetifikace_a_spr%C3%A1vy_informa%C4%8Dn%C3%ADch_aktiv.docx).



- National Institute of Standards and Technology. Framework for Improving Critical Infrastructure: Cybersecurity. Version 1.1. 16. dubna 2018.
- Návrh tzv. druhé cloudové vyhlášky. Dostupný z: <https://apps.odok.cz/veklep=-detail?pid-ALBSCDGK8LXB>.
- Návrh tzv. DORA nařízení, Nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a (EU) č. 909/2014, dostupný z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52020PC0595>.
- Návrh tzv. NIS2 směrnice, Směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148, dostupný z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=COM%3A2020%3A823%3AFIN>.
- Obecné pokyny Evropského orgánu pro bankovníctví (EBA) k oznamování významných incidentů podle směrnice PSD2. Dostupné z: <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2>.
- Pokyny Evropského orgánu pro bankovníctví EBA/GL/2019/02 zedne 25. února 2019. Dostupné z: [https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2761380/2b525e62-d8d7-4cc0-bd02-08f87a114f8a/EB%20revised%20Guidelines%20on%20outsourcing\\_CS.pdf?retry=1](https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2761380/2b525e62-d8d7-4cc0-bd02-08f87a114f8a/EB%20revised%20Guidelines%20on%20outsourcing_CS.pdf?retry=1).
- Standardy PCI DSS. Dostupné z: <https://www.pcistandard.cz/pcidss/>.
- Stanovisko Provozovatele informačního nebo komunikačního systému ze dne 10. března 2021. Dostupné z: [https://nukib.cz/download/publikace/podperne\\_materialy/Provozovatel-informacniho-nebo-komunikacniho-systemu\\_v3.1.pdf](https://nukib.cz/download/publikace/podperne_materialy/Provozovatel-informacniho-nebo-komunikacniho-systemu_v3.1.pdf).
- Stanovisko WP29, předchůdce současného Evropského sboru pro ochranu osobních údajů. Opinion 2/2017 on data processing at work. Dostupné z: <https://ec.europa.eu/newsroom/article29/items/610169/en>.
- Technical Guideline on Incident Reporting*. Dostupný z: <https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting>.
- The MITRE Corporation. MITRE ATT&CK: Design and Philosophy [online]. Dostupné z: [https://attack.mitre.org/docs/ATTACK\\_Design\\_and\\_Philosophy\\_March\\_2020.pdf](https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf).
- Úřední sdělení ČNB ze dne 8. ledna 2018 k hlášení bezpečnostních a provozních incidentů. Dostupné z: [https://www.cnb.cz/export/sites/cnb/cs/legislativa/.galleries/Vestnik-CNB/2018/vestnik\\_2018\\_02\\_20218320.pdf](https://www.cnb.cz/export/sites/cnb/cs/legislativa/.galleries/Vestnik-CNB/2018/vestnik_2018_02_20218320.pdf).
- What is a standard? World Standards Cooperation. Dostupný z: <https://www.worldstandards-cooperation.org/international-standards/international-standardseconomic-advantages/>.
- <https://csirt.cz/cs/hlaseni-incidentu/jak-ma-hlaseni-vypadat/>.
- [https://edpb.europa.eu/system/files/2022-01/edpb\\_guidelines\\_012021\\_pdbnotification\\_adopted\\_en.pdf](https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf).
- [https://oam.cnb.cz/sipresextdad/SIPRESEXT.www\\_forms.UVOD?p\\_lan=cs](https://oam.cnb.cz/sipresextdad/SIPRESEXT.www_forms.UVOD?p_lan=cs).
- [https://www.cnb.cz/export/sites/cnb/cs/platebni-styk/.galleries/pravni\\_predpisy/download/Postup-pro-podani-hlaseni-bezpecnostnich-a-provoznich-rizik.pdf](https://www.cnb.cz/export/sites/cnb/cs/platebni-styk/.galleries/pravni_predpisy/download/Postup-pro-podani-hlaseni-bezpecnostnich-a-provoznich-rizik.pdf).
- <https://www.ctu.cz/sites/default/files/obsah/ctu-new/formulare/oznamovaci-povinnost-a-evidence/metodicke-pokyny-k-zavaznemu-naruseni.docx>.



- <https://www.ctu.cz/sites/default/files/obsah/ctu-new/formulare/oznamovaci-povinnost-a-evidence/formular-oznameni-o-naruseni-bezpecnosti-a-ztrate-integrity.doc>.
- <https://www.isaca.org/>.
- <https://www.nist.gov/cyberframework/framework>.
- <https://www.nukib.cz/cs/kontakty/hlaseni-incidentu/>.
- [https://www.nukib.cz/download/publikace/formulare/Formular\\_incident\\_report\\_govcert.pdf](https://www.nukib.cz/download/publikace/formulare/Formular_incident_report_govcert.pdf).
- [https://www.nukib.cz/download/publikace/podpurne\\_materiály/2020-07-17\\_Minimalni-bezpecnostni-standard\\_v1.0.pdf](https://www.nukib.cz/download/publikace/podpurne_materiály/2020-07-17_Minimalni-bezpecnostni-standard_v1.0.pdf).
- <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305>.
- [www.csirt.cz](http://www.csirt.cz)
- [www.cnb.cz](http://www.cnb.cz)
- [www.nukib.cz](http://www.nukib.cz)
- ČSN EN ISO/IEC 27001:2014. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.
- ČSN ISO/IEC 27035-1:2018. *Informační technologie – Bezpečnostní techniky – Řízení incidentů bezpečnosti informací – Část 1: Principy řízení incidentů*. Praha: Česká agentura pro standardizaci, 2018.
- ČSN ISO/IEC 27035-2:2018. *Informační technologie – Bezpečnostní techniky – Řízení incidentů bezpečnosti informací – Část 2: Směrnice pro plánování a přípravu odezvy na incidenty*. Praha: Česká agentura pro standardizaci, 2018.
- ČSN ISO/IEC 27000:2020. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník*. Praha: Česká agentura pro standardizaci, 2020.
- ISO 37002:2021, *Whistleblowing management systems – Guidelines*.
- Metodika Nejvyššího státního zastupitelství, aplikace § 8 odst. 5 zák. o trestní odpovědnosti právnických osob.
- NIST 800-30 *Guide for Conducting Risk Assessments*.
- ISO 37301:2021, *Compliance management systems – Requirements with guidance for use*
- Standardy BS 25999 vydané British Standards Institute