Data Act

Nařízení (EU) 2023/2854

Přehledná shrnutí článků 1–40

Verze: Září 2025

Zpracoval:
Miroslav Kalinský, hlavní GDPR konzultant
EVERY REGARD s.r.o.

OBSAH

ČLÁNEK 1: PŘEDMĚT A OBLAST PŮSOBNOSTI 3
ČLÁNEK 2: DEFINICE 3
ČLÁNEK 3: OBECNÁ POVINNOST UMOŽNIT PŘÍSTUP K DATŮM 3
ČLÁNEK 4: PRÁVA UŽIVATELE 3
ČLÁNEK 5: POVINNOSTI VÝROBCE A POSKYTOVATELE 3
ČLÁNEK 6: PŘEDÁVÁNÍ DAT TŘETÍM STRANÁM 3
ČLÁNEK 7: OCHRANA PRÁV A ZÁJMŮ PŘIJÍMAJÍCÍCH STRAN 3
ČLÁNEK 8: VÝJIMKY Z POVINNOSTI ZPŘÍSTUPNIT DATA 4
ČLÁNEK 9: PODMÍNKY PRO ZPŘÍSTUPNĚNÍ DAT 4
ČLÁNEK 10: NÁKLADY SPOJENÉ S POSKYTOVÁNÍM DAT 4
ČLÁNEK 11: POVINNOSTI TŘETÍCH STRAN 4
ČLÁNEK 12: ZVLÁŠTNÍ PRAVIDLA PRO MIKROPODNIKY A MALÉ PODNIKY 4
ČLÁNEK 13: OCHRANA PŘED NEZÁKONNÝM PŘÍSTUPEM A VYUŽITÍM DAT 4
ČLÁNEK 14: OCHRANA OBCHODNÍHO TAJEMSTVÍ 5
ČLÁNEK 15: OCHRANA OSOBNÍCH ÚDAJŮ 5
ČLÁNEK 16: ZÁVAZNÉ MODELOVÉ SMLUVNÍ PODMÍNKY 5
ČLÁNEK 17: NEPLATNOST NESPRAVEDLIVÝCH SMLUVNÍCH PODMÍNEK 5
ČLÁNEK 18: PŘÍSTUP VEŘEJNÝCH ORGÁNŮ K DATŮM V PŘÍPADĚ VÝJIMEČNÉ POTŘEBY 5
ČLÁNEK 19: POSTUP PŘI POSKYTOVÁNÍ DAT VEŘEJNÝM ORGÁNŮM 5
ČLÁNEK 20: ODMĚNA ZA ZPŘÍSTUPNĚNÍ DAT VEŘEJNÝM ORGÁNŮM 6
ČLÁNEK 21: OBECNÉ ZÁSADY INTEROPERABILITY 6
ČLÁNEK 22: POVINNOSTI POSKYTOVATELŮ DATOVÝCH SLUŽEB V OBLASTI PŘENOSITELNOSTI 6
ČLÁNEK 23: POVINNOSTI POSKYTOVATELŮ PŘI VÝPOVĚDI SMLOUVY 6
ČLÁNEK 24: TECHNICKÉ POŽADAVKY NA PŘENOSITELNOST 6
ČLÁNEK 25: DOBROVOLNÁ SCHÉMATA CERTIFIKACE 6
ČLÁNEK 26: OBECNÉ POŽADAVKY NA INTEROPERABILITU CHYTRÝCH SMLUV 7
ČLÁNEK 27: POŽADAVKY NA BEZPEČNÉ VYPNUTÍ CHYTRÉ SMLOUVY 7
ČLÁNEK 28: OBECNÉ ZÁSADY PŘÍSTUPU VEŘEJNÝCH ORGÁNŮ K DATŮM OD SUBJEKTŮ JINÝCH NEŽ PODNIKY 7
ČLÁNEK 29: ZVLÁŠTNÍ USTANOVENÍ O PŘÍSTUPU VEŘEJNÝCH ORGÁNŮ K ÚDAJŮM 7
ČLÁNEK 30: SPOLUPRÁCE MEZI VEŘEJNÝMI ORGÁNY 7
ČLÁNEK 31: OCHRANNÁ OPATŘENÍ A DŮVĚRNOST PŘI PŘÍSTUPU VEŘEJNÝCH ORGÁNŮ K DATŮM 7
ČLÁNEK 32: ZPRÁVA O MIMOŘÁDNÉM PŘÍSTUPU VEŘEJNÝCH ORGÁNŮ K DATŮM 8
ČLÁNEK 33: EVROPSKÁ RADA PRO DATA 8
ČLÁNEK 34: OZNAMOVÁNÍ PORUŠENÍ POVINNOSTÍ 8
ČLÁNEK 35: POVINNOSTI PŘI UCHOVÁVÁNÍ DOKUMENTACE A AUDITECH 8
ČLÁNEK 36: SANKCE A VYMÁHÁNÍ 8
ČLÁNEK 37: ZMĚNY JINÝCH PRÁVNÍCH PŘEDPISŮ 8
ČLÁNEK 38: ZPRÁVY A PŘEZKUM 8
ČLÁNEK 39: VSTUP V PLATNOST A POUŽITELNOST 9
ČLÁNEK 40: ADRESÁTI 9

Článek 1: Předmět a oblast působnosti

Vymezuje hlavní cíl nařízení – podpořit spravedlivý přístup k datům a jejich využívání napříč EU. Upravuje přístup k datům generovaným produkty a službami připojenými k internetu. Nařízení se vztahuje na osobní i neosobní data a respektuje GDPR. Zahrnuje i interoperabilitu služeb a přístup veřejných orgánů v případě výjimečné potřeby. Stanoví rámec, ve kterém Data Act působí.

Článek 2: Definice

Zavádí klíčové pojmy používané v nařízení, včetně 'data', 'uživatel', 'výrobce', 'poskytovatel datových služeb' apod. Vymezuje produkty, služby a povahu generovaných dat. Rozlišuje osobní a neosobní data a definuje pravidla pro jejich nakládání. Důležité pro správné pochopení všech dalších článků. Tvoří právní slovník Data Actu.

Článek 3: Obecná povinnost umožnit přístup k datům

Výrobci a poskytovatelé musí umožnit uživatelům přístup k datům generovaným používáním produktů/služeb. Data musí být poskytnuta včas, ve strojově čitelné podobě a férově. Nesmí být zadržována z technických nebo smluvních důvodů. Základní ustanovení pro otevřený přístup k datům. Podporuje datovou transparentnost.

Článek 4: Práva uživatele

Uživatel má právo na přístup a další využívání dat. Může určit třetí stranu, která jeho data obdrží. Musí být informován o svých právech jasným způsobem. Umožňuje uživatelům využívat jejich data např. pro služby nebo analýzy. Zvyšuje kontrolu uživatele nad jeho daty.

Článek 5: Povinnosti výrobce a poskytovatele

Výrobci a poskytovatelé musí data poskytovat transparentně a nediskriminačně. Musí informovat uživatele o rozsahu a typu dat. Nesmějí bránit sdílení dat s třetími stranami. Mají povinnost chránit citlivá data a osobní údaje. Cílem je rovnováha mezi ochranou a dostupností dat.

Článek 6: Předávání dat třetím stranám

Uživatel může určit třetí stranu, které budou data zpřístupněna. Poskytování dat třetí straně musí být provedeno za stejných podmínek, jako by byla data poskytována samotnému uživateli. Třetí strana nesmí data zneužít a musí respektovat omezení stanovená uživatelem. Výrobce nebo poskytovatel služby nesmí takové předání blokovat. Cílem článku je usnadnit inovaci a konkurenci prostřednictvím sdílení dat.

Článek 7: Ochrana práv a zájmů přijímajících stran

Přijímající třetí strana má právo používat data v souladu s dohodou s uživatelem. Zároveň má povinnost chránit data před neoprávněným přístupem nebo zneužitím. Třetí strana nesmí poskytovat získaná data dalším subjektům bez souhlasu. Článek vyvažuje práva uživatele s ochranou zájmů třetích stran. Zajišťuje důvěru v datové ekosystémy.

Článek 8: Výjimky z povinnosti zpřístupnit data

Výrobce nebo poskytovatel služby nemusí zpřístupnit data v případě ochrany bezpečnosti, práv duševního vlastnictví nebo obchodního tajemství. Musí však prokázat, že rizika nelze přiměřeně zmírnit jiným způsobem. Nesmí se však jednat o svévolné odmítnutí přístupu. Výjimky musí být zdůvodněné a specifické. Článek chrání citlivé zájmy a motivuje k vyváženému přístupu.

Článek 9: Podmínky pro zpřístupnění dat

Data musí být poskytována ve standardizované a strojově čitelné podobě. Předání má být efektivní a bez zbytečných překážek. Formáty dat musí být přizpůsobeny technickým možnostem uživatele nebo třetí strany. Upravuje také formu, způsob a technická rozhraní pro přenos dat. Zajišťuje praktickou proveditelnost práva na přístup k datům.

Článek 10: Náklady spojené s poskytováním dat

Data musí být uživateli poskytována bezplatně, pokud se jedná o základní přístup. V případě, že o data žádá třetí strana, mohou být účtovány přiměřené náklady. Tyto náklady však nesmí být diskriminační nebo neodůvodněně vysoké. Cílem je zabránit zneužití poplatků k omezení přístupu k datům. Podporuje rovnováhu mezi přístupem k datům a náklady na jejich zpřístupnění.

Článek 11: Povinnosti třetích stran

Třetí strany, které získají přístup k datům od uživatele, jsou povinny s nimi nakládat v souladu s tímto nařízením. Musí respektovat účel, pro který byla data zpřístupněna, a nesmí je používat ke konkurenčním účelům vůči poskytovateli dat. Třetí strany nesmí pokusit se data zpřístupnit dalším osobám bez oprávnění. Mají také povinnost chránit data před neoprávněným přístupem. Článek zajišťuje odpovědné a bezpečné zacházení s daty v rukou příjemců.

Článek 12: Zvláštní pravidla pro mikropodniky a malé podniky

Mikropodniky a malé podniky mohou být za určitých podmínek vyňaty z některých povinností dle Data Actu. Výjimky se týkají především povinnosti zpřístupnit data třetím stranám. Toto ustanovení má za cíl zabránit neúměrnému zatížení menších subjektů. Zároveň však platí, že pokud takový podnik jedná jménem větší společnosti, výjimka se neuplatní. Článek zavádí ochranný mechanismus pro malé ekonomické subjekty.

Článek 13: Ochrana před nezákonným přístupem a využitím dat

Nařízení stanovuje povinnost přijímat technická a organizační opatření k ochraně dat před neoprávněným přístupem. Zahrnuje to i povinnost nevyužívat přístup k datům k získání konkurenční výhody. Porušení těchto povinností může vést k právním následkům, včetně odpovědnosti za škodu. Článek podporuje důvěru mezi subjekty, které si data vzájemně zpřístupňují. Předchází zneužívání datových toků v obchodních vztazích.

Článek 14: Ochrana obchodního tajemství

Pokud data obsahují obchodní tajemství, jejich sdílení musí být chráněno odpovídajícími opatřeními. Strany se musí dohodnout na způsobu zachování důvěrnosti těchto informací. Sdílení nesmí vést k odhalení chráněných know-how, pokud by to poškodilo oprávněné zájmy držitele tajemství. Nařízení požaduje rovnováhu mezi právem na přístup k datům a ochranou obchodních informací. Článek podporuje bezpečné datové prostředí i při sdílení citlivých údajů.

Článek 15: Ochrana osobních údajů

Při jakémkoli sdílení dat musí být respektována pravidla GDPR. Osobní údaje lze poskytovat pouze tehdy, pokud k tomu existuje právní základ a jsou dodrženy zásady zpracování. Subjekty musí zajistit transparentnost, minimalizaci údajů a bezpečnost při přenosu. Nařízení výslovně potvrzuje přednost právní úpravy ochrany osobních údajů. Tento článek zajišťuje soulad mezi Data Actem a ochranou soukromí jednotlivců.

Článek 16: Závazné modelové smluvní podmínky

Evropská komise může přijmout závazné modelové smluvní podmínky, které stanoví spravedlivé podmínky pro přístup k datům. Tyto podmínky budou mít za cíl ochránit slabší smluvní strany, zejména malé podniky. Modelové podmínky mohou být využívány dobrovolně nebo na základě povinnosti stanovené nařízením. Cílem je zabránit zneužití dominantního postavení při vyjednávání o přístupu k datům. Nařízení tak podporuje férové smluvní vztahy v datové ekonomice.

Článek 17: Neplatnost nespravedlivých smluvních podmínek

Smluvní podmínky, které jsou jednostranně vnuceny a které jsou nepřiměřeně nevýhodné, jsou považovány za neplatné. Toto ustanovení chrání zejména malé a střední podniky před zneužitím jejich slabšího postavení. Hodnotí se zejména rovnováha práv a povinností mezi stranami a průhlednost dané podmínky. Neplatnost se týká konkrétní doložky, nikoli celé smlouvy. Článek tak posiluje ochranu podnikatelského prostředí a transparentnost.

Článek 18: Přístup veřejných orgánů k datům v případě výjimečné potřeby

Ve výjimečných situacích, jako jsou přírodní katastrofy nebo mimořádné události, mohou veřejné orgány žádat přístup k datům. Takový přístup musí být nezbytný, časově omezený a přiměřený účelu. Žádost musí být řádně odůvodněná a poskytovatel dat má povinnost reagovat. Cílem je zajistit veřejný zájem a koordinaci v krizových situacích. Tento článek zajišťuje rovnováhu mezi ochranou dat a potřebami veřejné správy.

Článek 19: Postup při poskytování dat veřejným orgánům

Stanoví formální proces, kterým mají veřejné orgány žádat o přístup k datům. Obsahuje požadavky na písemnou žádost, její odůvodnění a specifikaci požadovaných dat. Zajišťuje také práva poskytovatelů dat, včetně možnosti odmítnutí, pokud žádost nesplňuje podmínky. Transparentní proces má zvýšit důvěru v legitimitu požadavků veřejných institucí. Článek zajišťuje právní jistotu a předvídatelnost při mimořádném přístupu ke komerčním datům.

Článek 20: Odměna za zpřístupnění dat veřejným orgánům

Poskytovatelé dat mají právo na přiměřenou finanční náhradu za zpřístupnění dat veřejnému orgánu. Odměna se stanovuje s ohledem na náklady, složitost a technické prostředky potřebné k poskytnutí dat. Ve výjimečných případech lze data poskytnout i bezplatně, pokud je to nezbytné pro zajištění základních veřejných služeb. Odměna musí být spravedlivá a nediskriminační. Tento článek chrání ekonomické zájmy poskytovatelů dat při mimořádném využití jejich infrastruktury.

Článek 21: Obecné zásady interoperability

Článek stanovuje obecné principy interoperability mezi poskytovateli datových služeb. Cílem je umožnit přenositelnost dat, aplikací a digitálních aktiv mezi různými systémy bez překážek. Poskytovatelé služeb musí zajistit technickou a smluvní kompatibilitu. Zároveň se podporuje využívání otevřených standardů a rozhraní. Interoperabilita je klíčová pro otevřený a konkurenceschopný datový trh.

Článek 22: Povinnosti poskytovatelů datových služeb v oblasti přenositelnosti

Poskytovatelé služeb musí umožnit svým zákazníkům přenos dat a digitálních aktiv ke konkurenci. Musí odstranit technické, smluvní a obchodní překážky, které by takovému přechodu bránily. Přechod musí být možný v přiměřené lhůtě a bez výpadků nebo ztráty dat. Zákazníci nesmějí být penalizováni za přechod k jinému poskytovateli. Článek podporuje uživatelskou svobodu a konkurenci mezi cloudovými službami.

Článek 23: Povinnosti poskytovatelů při výpovědi smlouvy

Pokud zákazník ukončí smlouvu s poskytovatelem datové služby, musí mu být umožněn bezpečný výstup dat. Zahrnuje to i přenos metadat, nastavení a uživatelských oprávnění. Zákazník musí být informován o způsobu, formátu a nákladech na výstup dat. Tím se předchází tzv. vendor lock-in, tedy závislosti na jednom poskytovateli. Článek chrání právo zákazníka svobodně volit digitální služby.

Článek 24: Technické požadavky na přenositelnost

Evropská komise může vydat prováděcí akty určující technické specifikace, které zajistí skutečnou přenositelnost služeb. Tyto požadavky mohou zahrnovat formáty dat, aplikační rozhraní, bezpečnostní protokoly apod. Poskytovatelé musí zajistit kompatibilitu svých systémů s těmito požadavky. Díky tomu bude možné snadno přecházet mezi poskytovateli bez překážek. Článek zajišťuje technický základ pro praktickou interoperabilitu.

Článek 25: Dobrovolná schémata certifikace

Na podporu důvěry mezi poskytovateli a uživateli mohou být zavedena dobrovolná schémata certifikace. Certifikace potvrdí, že daný poskytovatel splňuje požadavky na interoperabilitu a přenositelnost. Zúčastněné subjekty mohou tímto způsobem prokázat svou transparentnost a důvěryhodnost. Certifikace může být využita i pro zjednodušení výběrových řízení a veřejných zakázek. Článek podporuje standardizaci a zvyšuje důvěru v digitální ekosystémy.

Článek 26: Obecné požadavky na interoperabilitu chytrých smluv

Chytré smlouvy musí být navrženy tak, aby byly interoperabilní s jinými systémy a procesy. To zahrnuje schopnost komunikace mezi systémy různých dodavatelů a technologií. Interoperabilita usnadňuje sdílení dat a jejich praktické využití napříč trhy. Vývojáři chytrých smluv musí brát ohled na otevřenost a kompatibilitu již při návrhu. Tento článek podporuje technickou soudržnost v prostředí digitálních služeb.

Článek 27: Požadavky na bezpečné vypnutí chytré smlouvy

Chytré smlouvy musí obsahovat funkce umožňující jejich bezpečné a úplné vypnutí. Cílem je chránit uživatele v případě zneužití, technické chyby nebo právního zásahu. Vypnutí musí být provedeno tak, aby nedošlo ke ztrátě důležitých údajů. Tato povinnost se vztahuje především na poskytovatele, kteří chytré smlouvy zpřístupňují. Článek zajišťuje vyšší bezpečnost a kontrolu v oblasti automatizovaných digitálních smluv.

Článek 28: Obecné zásady přístupu veřejných orgánů k datům od subjektů jiných než podniky

Veřejné orgány mohou v mimořádných situacích žádat přístup k datům i od nepodnikatelských subjektů (např. neziskové organizace). Takový přístup je možný pouze tehdy, pokud není možné získat data od podnikatelských subjektů. Data musí být poskytnuta pouze v rozsahu nezbytném k dosažení veřejného zájmu. Tento přístup je podmíněn zásadami proporcionality a subsidiarity. Článek rozšiřuje možnosti krizového řízení za současného respektování práv subjektů.

Článek 29: Zvláštní ustanovení o přístupu veřejných orgánů k údajům

Tento článek upravuje detailní podmínky, za kterých mohou veřejné orgány přistupovat k datům subjektů. Musí existovat konkrétní právní základ a žádost musí být přiměřená a zdůvodněná. Veřejný orgán musí minimalizovat zásah do práv vlastníků dat. Poskytovatel dat může požádat o kompenzaci nákladů spojených s poskytnutím dat. Cílem je vytvořit vyvážený rámec pro mimořádný přístup ke komerčním a soukromým datům.

Článek 30: Spolupráce mezi veřejnými orgány

Veřejné orgány členských států a institucí EU musí spolupracovat při žádostech o přístup k datům. Mají povinnost si vzájemně poskytovat informace a podporu. Tato spolupráce pomáhá předejít duplicitním žádostem a zvyšuje efektivitu krizového řízení. Zároveň je zajištěna právní jistota a jednotný přístup napříč členskými státy. Článek podporuje koordinované využívání dat ve veřejném zájmu.

Článek 31: Ochranná opatření a důvěrnost při přístupu veřejných orgánů k datům

Veřejné orgány musí zavést ochranná opatření k zajištění důvěrnosti dat, ke kterým získají přístup. Tato opatření zahrnují technické a organizační prostředky na ochranu proti neoprávněnému přístupu, ztrátě či zneužití. Získaná data nesmí být použita k jiným účelům, než bylo původně stanoveno. Veřejné orgány jsou povinny vést záznamy o všech přístupech k datům. Cílem je zajistit důvěru subjektů poskytujících data v odpovědné zacházení s citlivými informacemi.

Článek 32: Zpráva o mimořádném přístupu veřejných orgánů k datům

Veřejné orgány, které využily přístup k datům na základě výjimečné potřeby, musí každoročně zveřejnit zprávu o těchto případech. Zpráva má obsahovat účel přístupu, typ dat, identitu poskytovatele a přijatá opatření k ochraně práv. Zajišťuje transparentnost a umožňuje veřejnou kontrolu mimořádného přístupu. Pomáhá odhalovat případná pochybení nebo zneužití. Článek podporuje otevřenost a odpovědnost veřejné správy při nakládání s daty.

Článek 33: Evropská rada pro data

Zřizuje se Evropská rada pro data jako poradní orgán složený ze zástupců členských států a Komise. Úkolem rady je podporovat konzistentní uplatňování Data Actu napříč EU. Rada bude vydávat stanoviska, doporučení a usměrnění k výkladu a praxi. Bude také sloužit jako fórum pro výměnu zkušeností mezi členskými státy. Cílem je podpořit jednotný a efektivní rámec správy dat v celé Unii.

Článek 34: Oznamování porušení povinností

Článek zavádí mechanismus pro oznamování porušení pravidel stanovených v Data Actu. Fyzické i právnické osoby mohou hlásit porušení příslušným orgánům členského státu. Oznamovatelé musí být chráněni před odvetnými opatřeními. Zavádí se také požadavek na zavedení důvěryhodných a anonymních kanálů. Podporuje efektivní vymáhání nařízení a ochranu veřejného zájmu.

Článek 35: Povinnosti při uchovávání dokumentace a auditech

Subjekty, které zpřístupňují nebo přijímají data, musí vést dokumentaci o těchto procesech. Dokumentace musí být uchovávána po stanovenou dobu a musí být přístupná pro účely kontroly. Příslušné orgány mohou provádět audity za účelem ověření souladu s nařízením. Cílem je zajistit zpětnou dohledatelnost, odpovědnost a transparentnost. Článek podporuje správné plnění povinností a efektivní dohled.

Článek 36: Sankce a vymáhání

Členské státy musí stanovit sankce za porušení tohoto nařízení. Sankce musí být účinné, přiměřené a odrazující. Orgány vymáhající pravidla musí mít dostatečné pravomoci a nástroje pro šetření. Součástí je i přeshraniční spolupráce mezi orgány členských států. Cílem je zajistit reálné dodržování Data Actu napříč EU.

Článek 37: Změny jiných právních předpisů

Tento článek uvádí změny, které Data Act provádí v jiných předpisech EU. Jedná se o úpravy zajišťující soulad a harmonizaci s existující legislativou. Změny se týkají zejména pravidel přenositelnosti a interoperability digitálních služeb. Zajišťují jednotné právní prostředí v oblasti dat. Cílem je sladit Data Act s širším rámcem digitální strategie EU.

Článek 38: Zprávy a přezkum

Evropská komise musí pravidelně předkládat zprávy o uplatňování tohoto nařízení. První zpráva musí být zveřejněna do tří let od nabytí účinnosti. Na základě těchto zpráv může Komise navrhnout úpravy nebo nové legislativní kroky. Přezkum se zaměřuje na účinnost, dopady a potřeby aktualizace. Článek zajišťuje, že Data Act zůstane funkční a aktuální v měnícím se digitálním prostředí.

Článek 39: Vstup v platnost a použitelnost

Data Act vstupuje v platnost dvacátým dnem po vyhlášení v Úředním věstníku EU. Použitelnost většiny ustanovení je odložena na 20 měsíců po vstupu v platnost, tedy do 12. září 2025. Toto přechodné období má umožnit subjektům přípravu na nové povinnosti. Datum vstupu v platnost je klíčové pro výklad časové účinnosti pravidel. Článek poskytuje právní jistotu ohledně účinnosti celého nařízení.

Článek 40: Adresáti

Nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech EU. Týká se podniků, institucí i orgánů veřejné správy. Členské státy mají povinnost zajistit vnitrostátní vykonatelnost pravidel. Tímto se nařízení stává právně účinným nástrojem jednotného digitálního trhu. Článek formálně uzavírá normativní část a potvrzuje obecnou platnost pravidel.

Poslední aktualizace: 6. září 2025