KOMORNÍ FILHARMONIE PARDUBICE

Sukova třída 1260, 530 02 Pardubice, IČ: 00088447

Interní směrnice č. 20
PRO NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI

GDPR

Směrnice pro nakládání s osobními údaji

1. PŘEDMĚT SMĚRNICE A ZÁKLADNÍ USTANOVENÍ

1.1. Touto směrnicí Komorní filharmonie Pardubice (dále jen „filharmonie“) stanovuje vnitřní pravidla pro zajištění ochrany osobních údajů a plnění povinností podle Obecného nařízení EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů jakožto přímo účinného předpisu EU (dále též „Obecné nařízení“) a podle zákona o zpracování osobních údajů (dále též „zákon“), zejména při zpracování osobních údajů vykonávaných Komorní filharmonií Pardubice.

1.2. Ustanovení této směrnice jsou závazná pro všechny osoby v rámci filharmonie, zejména pro zaměstnance.

1.3. Správcem osobních údajů je filharmonie v těch případech, kdy sama určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Může být správcem i při zpracování pomocných agend, které vede pro usnadnění své činnosti jako zpracovatel.

1.4. Pokud pro filharmonie zajišťuje zpracování osobních údajů v rámci plnění smluvních povinností jiný subjekt (zpracovatel), pak musí být v rámci smluvních vztahů zaručeno plnění povinností podle Obecného nařízení a podle této směrnice a musí být upravena odpovědnost za tyto činnosti vůči správci a vůči kontrolním orgánům. Náležitosti smlouvy o zpracování osobních údajů upravuje Obecné nařízení.

2. ZÁKLADNÍ POJMY

Základní pojmy ochrany osobních údajů stanovuje Obecné nařízení a zákon. V souladu s tím je

2.1. **osobním údajem** jakákoliv informace týkající se identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;

2.2. **citlivým osobním údajem** osobní údaj vypovídající rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Osobní údaje týkající se rozsudků v trestních věcech a trestných činů se pro účel této směrnice hodnotí obdobně jako citlivé osobní údaje.

2.3. **zpracováním osobních údajů** jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení; za zpracování osobních údajů se nepovažuje pořízení a použití jednotlivých fotografií nebo časově omezeného obrazového záznamu (schůze, kulturní, společenské, sportovní akce), aniž se vytváří evidence a nejsou kromě běžné identifikace jménem a příjmením systematicky přiřazovány další osobní údaje,

2.4. **subjektem údajů** fyzická osoba, k níž se osobní údaje vztahují,

2.5. **souhlasem subjektu údajů** jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.

3. OSOBNÍ ÚDAJE A JEJICH ZPRACOVÁNÍ

3.1. Způsob zpracování osobních údajů a pověřené osoby

3.1.1. Osobní údaje lze zpracovávat pouze za podmínek stanovených Obecným nařízením, případně zvláštními zákony, přičemž je nezbytné dodržovat ustanovení této směrnice. Zpracovávat lze pouze osobní údaje získané zákonným způsobem.

3.1.2. Zpracovávat osobní údaje a seznamovat se s nimi mohou v rozsahu podle následujících ustanovení pouze pověřené osoby, kterými jsou:

3.1.2.1. zaměstnanec, který v souladu se svým pracovním zařazením vykonává agendu, jejíž nezbytnou součástí je zpracování osobních údajů,

3.1.2.2. člen orgánu, pokud je to nezbytné pro výkon jeho funkce,

3.1.2.3. osoby, které k tomu mají oprávnění na základě uzavřené smlouvy.

3.2. Účel zpracování, zákonnost a nově zaváděné účely zpracování[1]

3.2.1. Ten, kdo rozhoduje o činnosti zpracování (dále „odpovědný zaměstnanec“), pro každé zpracování (agendu, evidenci) stanoví účel zpracování, tedy jeho výstižný a konkrétně vymezující popis v rozsahu několika slov. O účelu drobných zpracování (tj. zpracování s nízkým rizikem[2]) rozhoduje osoba, do jejíž kompetence spadá úkol, který zpracování osobních údajů vyžaduje. V případě, kdy lze předpokládat, že účel zpracování zasahuje subjekty osobních údajů ve velkém rozsahu, je povinna předložit stanovení účelu k rozhodnutí svému nadřízenému.

3.2.2. Právní titul či tituly [3] každého účelu zpracování určí odpovědný zaměstnanec. V případě, kdy agenda obsahuje také citlivé osobní údaje, určí zároveň právní titul pro citlivé údaje. K obojímu určí také právní základ, je-li potřebný.

3.2.3. Při potřebě nového zpracování osobních údajů ten, kdo navrhuje jeho účel, posoudí oprávněnost účelu, a navrhne nezbytný rozsahu údajů pro dané zpracování, dobu a způsob uchování a způsob informování subjektů údajů.

3.2.4. Ke stanovení účelu zpracování, určení právního titulu a případně právního základu si odpovědný zaměstnanec vyžádá posouzení pověřencem.

3.2.5. Pověřené osoby jsou povinny zpracovávat osobní údaje pouze ke stanovenému účelu, v rozsahu pracovní náplně a úkolů, které jim byly stanoveny jejich nadřízenými anebo vyplývajícím z jejich funkce, a na místech k tomu určených. Jsou povinny dodržovat základní zásady při zpracování osobních údajů.

3.2.6. Ustanovení tohoto článku se přiměřeně vztahuje i na člena orgánu při výkonu jeho funkce, který spolupracuje s odpovědným zaměstnancem a pověřencem.

3.3. Zásady zpracování osobních údajů

Základní zásady při zpracování osobních údajů jsou:

3.3.1. zpracovávat osobní údaje korektním a transparentním způsobem,

3.3.2. před zavedením každého zpracování osobních údajů stanovit účel, právní titul a případně právní základ či oprávněné důvody správce pro toto zpracování,

3.3.3. zpracovávat osobní údaje pouze v nezbytném rozsahu a po dobu nezbytnou k danému účelu,

3.3.4. zpracovávat osobní údaje přesné a podle potřeby je aktualizovat,

3.3.5. zajišťovat náležité zabezpečení osobních údajů.

3.4. Záznamy o zpracování a analýza osobních údajů

3.4.1. Ve spolupráci s pověřencem je vytvořena Analýza osobních údajů, dokládající soulad s Obecným nařízením. Výstupem analýzy jsou záznamy zpracování obhajující:

3.4.1.1. záznamy o příslušných účelech zpracování (dále jen „záznam o zpracování“)[4]

3.4.1.2. záznamy o provedených opatřeních k dosažení souladu s Obecným nařízením, jako je šifrování, likvidace či výmaz dat, lhůty pro likvidaci,

3.4.1.3. záznamy o bezpečnostních incidentech, jako je únik, ztráta, neoprávněný přenos či zveřejnění,

3.4.1.4. další údaje potřebné k vyhodnocení a doložení souladu s Obecným nařízením a k informování subjektů údajů.

3.4.2. K analýze osobních údajů mají přístup odpovědní zaměstnanci a pověřenec. Zaměstnanci vždy informují pověřence o změnách zpracování osobních údajů. Pověřenec na základě informací provede změny v analýze osobních údajů.

3.4.3. Vedoucí osoba nebo jím určená osoba zajistí pravidelné zálohování analýzy osobních údajů a případných souvisejících dokladů.

4. Doklady o souladu s Obecným nařízením

4.1. Každá pověřená osoba, pokud to plyne z náplně její práce, dbá na uchování dokladů, opravňujících určité zpracování osobních údajů, jako jsou

4.1.1. smlouvy, pro jejichž plnění se zpracovávají osobní údaje,

4.1.2. doklady o informování subjektů údajů v případech, kdy nepostačuje zveřejnění na webu,

---

[1] Čl. 5 odst. 1 písm. a) a b) Obecného nařízení

[2] Čl. 33 odst. 1 ON, případy, kdy není pravděpodobné, že by porušení zabezpečení mělo za následek riziko pro práva a svobody fyzických osob

[3] Právním titulem je některé ustanovení čl. 6 odst. 1 písm. a) až f), čl. 9/2 písm. a) až j), čl. 10 Obecného nařízení.

[4] Čl. 30 Obecného nařízení

4.1.3. doklady o vyřízení žádostí subjektů údajů,
4.1.4. souhlasy se zpracováním osobních údajů,
4.1.5. balanční testy v případě zpracování na základě právního titulu oprávněného zájmu správce nebo třetí osoby,
4.1.6. evidence klíčů,
4.1.7. evidence přístupů do počítačů a přístupových práv v informačním systému,
4.1.8. údaje o zpřístupnění záznamu kamerového systému či dalších specifických záznamů osobních údajů,
4.1.9. další obdobné doklady.

5. PRÁVA SUBJEKTŮ ÚDAJŮ

5.1. Informování subjektů údajů[5]

5.1.1. Odpovědný zaměstnanec zajistí informování subjektů údajů, jejichž údaje filharmonie zpracovává, zejména na webu filharmonie, případně při uzavření smlouvy nebo získání souhlasu se zpracováním. Zajistí též stručný, transparentní, srozumitelný a snadno přístupný způsob těchto sdělení[6].

5.1.2. Odpovědný zaměstnanec zajistí také doložitelnost uvedeného informování. Může v rámci své kompetence tento úkol uložit jinému zaměstnanci.

5.2. Přístup k osobním údajům[7]

5.2.1. Požadavky subjektů údajů vyřizuje odpovědný zaměstnanec. Může v rámci své kompetence tento úkol uložit jinému zaměstnanci.

5.2.2. Požádá-li subjekt údajů o sdělení svých osobních údajů, ověří se totožnost žadatele a potvrdí na žádosti, případně se ověření totožnosti k žádosti přiloží, např. číslo průkazu, podle kterého byla ověřena, ověření uznávaného elektronického podpisu, datové schránky (dále jen „ověření totožnosti“).

5.2.3. Běžné provozní dotazy týkající se osobních údajů (zejm. informace o zpracování osobních údajů), vyřídí zaměstnanec obratem.

5.2.4. K vyřízení ostatních žádosti o přístup k osobním údajům (zejm. export údajů) je příslušný odpovědný zaměstnanec. Žádost se vyřídí do 30 dnů.

5.2.5. V případě potřeby a s ohledem na složitost a počet žádostí může odpovědný zaměstnanec prodloužit lhůtu vyřízení žádosti o další dva měsíce, přičemž o tom informuje subjekt údajů do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad.

5.2.6. Jestliže subjekt údajů podává žádost v elektronické formě a je-li to možné, poskytnou se informace v elektronické formě, pokud subjekt údajů nepožádá o jiný způsob.

5.2.7. Požadavky subjektů údajů, přenos osobních údajů a další dotazy ohledně zpracování osobních údajů vždy zaměstnanci konzultují s pověřencem na ochranu osobních údajů.

5.3. Právo na výmaz, opravu a doplnění

5.3.1. Pověřené osoby jsou povinny dbát na správnost zpracovávaných osobních údajů.

5.3.2. Subjekt údajů má právo žádat výmaz, opravu a doplnění osobních údajů, které se ho týkají.[8] Případy, kdy je požadavek na výmaz oprávněný, stanoví čl. 17 odst. 1 a 3 Obecného nařízení. Žádost vyřídí odpovědný zaměstnanec po ověření totožnosti a po prověření oprávněnosti požadavku ihned, jakmile je to možné, nejdéle do 30 dnů; čl. 5.2.5. Směrnice se použije obdobně. Pokud má ověření oprávněnosti požadavku trvat delší dobu, zejména by se osobní údaje dotčené žádostí měly zpracovávat ke stanovenému účelu zpracování (např. zaslat pravidelné vyúčtování s chybným údajem), zajistí jejich vyřazení ze zpracování [9] a informuje o tom žadatele. Ve složitých případech si vyžádá posouzení pověřencem.

5.3.3. Oznámí-li subjekt údajů (např. telefonicky nebo emailem), že osobní údaje, které se ho týkají, se změnily, a nelze dostatečně ověřit jeho totožnost s ohledem na závažnost požadované změny (např. na základě osobní znalosti hlasu, znalosti e-mailové adresy), vyzve ho odpovědný zaměstnanec k postupu, umožňujícímu totožnost ověřit.

---

[5] Čl. 13 a 14 Obecného nařízení.
[6] Čl. 12 Obecného nařízení
[7] Čl. 15 Obecného nařízení
[8] Čl. 16, 17 Obecného nařízení
[9] „omezení zpracování“

5.3.4. Zjistí-li pověřená osoba při své činnosti, že při zpracování osobních údajů došlo ke zjevné chybě v psaní (např. překlepu), informuje odpovědného zaměstnance a údaj opraví.

6. POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

6.1. Vedoucí osoba zajistí zveřejnění kontaktních údajů pověřence a Úřadu pro ochranu osobních údajů je sdělí včetně jeho identifikace.

6.2. Všechny pověřené osoby jsou povinny [10]:

6.2.1. konzultovat s pověřencem všechny záležitosti, související s ochranou osobních údajů, pokud si nejsou zcela jisty jejich prováděním v souladu s Obecným nařízením,

6.2.2. poskytnout pověřenci součinnost při plnění jeho úkolů, zejména mu umožnit plný přístup k osobním údajům a k operacím zpracování,

6.2.3. zdržet se jakéhokoli jednání, které by mohlo ohrozit nezávislé posouzení věci pověřencem,

6.2.4. neukládat pověřenci úkoly, které by vedly k jeho střetu zájmů.

6.3. Povinnosti pověřence jsou stanoveny ve zvláštní smlouvě.

7. BEZPEČNOST INFORMACÍ

7.1. Obecné postupy při zabezpečení osobních údajů

7.1.1. Přiměřeně zabezpečeny musejí být zpracovávané osobní údaje i ty, které nejsou systematicky zpracovávané, například vyskytující se v jednotlivých nezařazených dopisech, sděleních, e-mailech.

7.1.2. Úroveň zabezpečení lze přiměřeně snížit u osobních údajů, u nichž je riziko pro subjekty údajů nepatrné nebo jsou běžně dostupné veřejnosti, zejména o zaměstnancích a členech orgánů, dalších osobách

7.1.2.1. na základě zákona o svobodném přístupu k informacím,

7.1.2.2. jsou veřejně dostupné (například ve veřejně přístupných registrech),

7.1.2.3. nepředstavují žádné riziko pro subjekty údajů, například malý počet nahodilých nevýznamných informací.

7.1.3. V pochybnostech je pověřená osoba vždy povinna konzultovat potřebu zabezpečení s nadřízeným nebo s pověřencem.

7.1.4. Osobní údaje musí být zabezpečeny před neoprávněným nebo nahodilým přístupem k nim, proti jejich změně, zničení či ztrátě (zejména dostatečné zálohování), neoprávněným a nezabezpečeným přenosům, proti jejich jinému neoprávněnému zpracování, jakož i proti jinému zneužití osobních údajů. Zabezpečení spočívá při nepřítomnosti pověřených osob zejména v uchovávání záznamových médií (písemných i elektronických), obsahujících osobní údaje, v uzamčených skříních, v uzamykání kanceláří a jiných míst a dále v dodržování pravidel informační bezpečnosti.

7.1.5. Dále jsou pověřené osoby povinny vyvarovat se jakéhokoliv jednání, které by mohlo být chápáno jako neoprávněné zveřejňování osobních údajů, nebo vést k neoprávněnému přístupu třetích osob k osobním údajům. Zejména, ale nikoliv pouze:

7.1.5.1. sdělovat jakékoliv osobní údaje jiné osobě, než která je subjektem údajů nebo je jejím zákonným zástupcem,

7.1.5.2. hlasitě sdělovat osobní údaje ve veřejně přístupných prostorách

7.1.5.3. umožnit nepovolaným osobám nahlížet do listin, které nesou osobní údaje, nebo na obrazovku monitoru, kde jsou takové údaje zobrazeny,

7.1.5.4. sdělovat komukoliv svá přístupová hesla do počítače, do informačních systémů a hesla k zašifrovaným souborům nebo zařízením.

7.2. Zabezpečení písemností a záznamových médií obsahujících osobní údaje

7.2.1. Písemnosti a digitální záznamová média, které obsahují osobní údaje, musí být mimo dobu, kdy jsou pod dohledem zaměstnanců, zabezpečeny v uzamčených skříních, popř. na jiných místech, zajišťujících jejich ochranu. To platí i pro kopie písemností a digitální zálohy, obsahující osobní údaje.

7.2.2. Za plnění povinností stanovených ve výše uvedených odstavcích tohoto článku jsou odpovědny pověřené osoby podle rozsahu svých oprávnění.

[10] Čl. 38 Obecného nařízení

7.3. Zabezpečení dat obsahujících osobní údaje v osobních počítačích a na sítích

7.3.1. Data obsahující osobní údaje, která jsou uložena v osobních počítačích, musí být zabezpečena před volným přístupem neoprávněných osob, před změnou, zničením, ztrátou, neoprávněnými přenosy, jiným neoprávněným zpracováním, jakož i jiným zneužitím osobních údajů.

7.3.2. Pevné počítače s přístupem k osobním údajům musejí mít alespoň zabezpečený přístup do počítače (přihlášení pod heslem) a nastaveno uzamčení obrazovky po době nečinnosti nejvýše 3 minuty.

7.3.3. Významné evidence osobních údajů (například mzdová, personální agenda a další rozsáhlá evidence) musejí být zabezpečeny také zvláštním přístupem do programového vybavení anebo být jako soubor šifrované.

7.3.4. Data s osobními údaji na jakémkoliv přenosném médiu, jako je notebook, flashdisk, přenosný disk, uložiště souborů mobilního telefonu a podobně, musejí být zajištěny alespoň:

7.3.4.1. Šifrováním disku či jiného uložiště pomocí šifrovacího programu,

7.3.4.2. zabezpečeným přístupem do programového vybavení, které data ukládá šifrovaně,

7.3.4.3. být jako soubor šifrované, nebo

7.3.4.4. je-li to dostatečné s ohledem na riziko pro subjekty osobních údajů, být dostatečně pseudonymizovány.

7.3.5. Pověřené osoby pravidelně posuzují úroveň zabezpečení informačních systémů včetně přenosu dat s ohledem na rizika pro subjekty osobních údajů, a v případě potřeby přijímají vhodná technická a organizační opatření, aby rizika zmírnily.[11]

7.3.6. Pověřené osoby zejména dbají na dostatečnou kvalitu hesel (nejméně 8 znaků, obsahuje minimálně 3 ze 4 položek: Velká písmena, malá písmena, čísla, symboly jako pomlčka či lomítko), pravidelné obměny hesel a je-li to možné vzhledem k nutné zastupitelnosti, důvěrnosti pouze pro jednoho uživatele. V případě potřeby ukládají hesla zabezpečeně a zcela odděleně od počítačů a médií, na nichž jsou použita.

7.3.7. Přenos souborů s osobními údaji nezabezpečenou sítí Internet (např. protokol http:/) a jejich uložení na nezabezpečených uložištích (běžné e-mailové schránky, přechodná uložiště jako Úschovna.cz) je přípustný jen se zašifrováním souboru a předáním hesla příjemci jinou cestou, například SMS zprávou na ověřené číslo telefonu či pomocí jiné bezpečné aplikace.

7.3.8. Za plnění povinností stanovených v tomto článku jsou odpovědny pověřené osoby podle rozsahu svých oprávnění.

8. Porušení zabezpečení a míra jeho rizika

8.1. Zjistí-li kdokoliv, že došlo k fyzickému nebo elektronickému porušení zabezpečení osobních údajů, například úniku, ztrátě, zničení, neoprávněnému zveřejnění osobních údajů (dále jen „incident“), neprodleně o tom informuje odpovědného zaměstnance a pověřence.

8.2. Odpovědný zaměstnanec vyhodnotí riziko pro práva a svobody fyzických osob, a konzultuje s pověřencem. Pokud ve shodě s pověřencem posoudí jako nepravděpodobné, že by incident měl za následek riziko pro práva a svobody fyzických osob (dále jen „nízké riziko“), provede pověřenec o incidentu záznam k příslušnému účelu zpracování v analýze osobních údajů. Pokud vyhodnotí, že nejde jen o nízké riziko, ohlásí tuto skutečnost Úřadu pro ochranu osobních údajů nejpozději do 72 hodin od okamžiku, kdy se o porušení zabezpečení dozvěděl některý odpovědný zaměstnanec.[12]

8.3. Pokud je riziko pro práva a svobody fyzických osob vysoké, odpovědný zaměstnanec ve spolupráci s pověřencem vhodným způsobem informuje subjekty údajů.[13] Pokud v konzultaci s pověřencem však vyhodnotí, že již existuje či lze přijmout opatření, díky němuž se vysoké riziko pro subjekty údajů neprojeví, anebo by informování vyžadovalo nepřiměřené úsilí, pouze zveřejní informaci o incidentu na webu obce na výrazném místě.

9. ZÁVĚREČNÁ USTANOVENÍ

9.1. Kontrola dodržování směrnice

9.1.1. Vedoucí osoba zajistí kontrolu plnění povinností vyplývajících z ustanovení Směrnice pro nakládání s osobními údaji.

[11] Čl. 32 Nařízení
[12] Čl. 33 Nařízení
[13] Čl. 34 Nařízení

9.1.2. Ředitel filharmonie zajistí, aby byli s dokumentem Směrnice pro nakládání s osobními údaji seznámeni všechny pověřené osoby, další zaměstnanci a dodavatelé, kteří mohou přijít jakýmkoliv způsobem do styku s osobními kontakty.

9.2. Revize směrnice

9.2.1. Revize Směrnice pro nakládání s osobními údaji je provedena v případě potřeby, minimálně však jednou za dva roky.

9.2.2. Za zpracování, údržbu a revize Směrnice pro nakládání s osobními údaji odpovídá ředitel filharmonie nebo jím pověřená osoba.

9.2.3. Revize směrnice se provádí na základě konzultace s pověřencem pro ochranu osobních údajů.

9.3. Účinnost směrnice

Směrnice pro nakládání s osobními údaji nabývá účinnosti a platnosti dnem vydání a zároveň zrušuje Interní směrnici č. 20 O NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI filharmonie ze dne 31.5.2018.

V Pardubicích, dne 2.10.2023

MgA. Pavel Svoboda, Ph.D. – ředitel v.r.