ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 555, fax: 234 665 444
e-mail: posta@uoou.cz, www.uoou.cz

Čj. UOOU-07399/18-62
Praha 15. dubna 2019

PROTOKOL O KONTROLE

Kontrolní orgán:
Úřad pro ochranu osobních údajů, se sídlem 170 00 Praha – Holešovice, Pplk. Sochora 727/27, IČ: 70837627 (dále jen „Úřad“).

Pravomoc kontrolního orgánu k výkonu kontroly vyplývá z čl. 58 odst. 1 písm. b) 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) zároveň v souladu s § 2 odst. 2 a 3 a § 29 odst. 1 písm. a) zákona č. 101/2000 Sb.

Kontrolující:

PaedDr. Jana Rybínová – inspektorka Úřadu pro ochranu osobních údajů;
JUDr. Michal Jelínek – pověřený zaměstnanec Úřadu pro ochranu osobních údajů; Ing. Max Gůt – pověřený zaměstnanec Úřadu pro ochranu osobních údajů.

Kontrolovaná osoba:

Státní ústav pro kontrolu léčiv se sídlem Šrobárova 48, 100 41 Praha 10, IČ: 00023817 (dále také „SÚKL“, „Kontrolovaná osoba“ nebo „Ústav“).

Zastoupená:

Ing. Zdeněk Kusovský, MBA, Manager bezpečnosti informací, pověřenec pro ochranu osobních údajů – pověření k zastupování SÚKL ze dne 8. srpna 2018, příloha č.j. UOOU-07399/18-5; pověření Pověřence pro ochranu osobních údajů v SÚKL ze dne 12. 7. 2017 – příloha č.j. UOOU-07399/18-2).

Místo provedení kontroly:

Sídlo Úřadu pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7;
Sídlo Státního ústavu pro kontrolu léčiv, Šrobárova 48, 100 41 Praha 10;
Sídlo XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX;
Sídlo společnosti XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

Předmět kontroly:

Předmětem kontroly je dodržování povinností stanovených v Nařízení (EU) 2016 v souvislosti se zpracováním osobních údajů v Centrálním úložišti elektronických receptů (dále také „CÚeR“), vedeného podle § 81 zákona č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech), a to v návaznosti na zavedení povinnosti vydávat elektronické recepty (od 1. ledna 2018) a s tím související rozsáhlé zpracování osobních údajů, zejména kontrola zabezpečení osobních údajů při tomto zpracování.

Zahájení kontroly: přípis Oznámení o zahájení kontroly č.j. UOOU- 07399/18-4 ze dne 30. července 2018, které Kontrolovaná osoba obdržela do datové schránky téhož dne.

Poslední kontrolní úkon: předcházející vyhotovení protokolu o kontrole – Úřední záznam – vložení dokumentů do spisové dokumentace, ze dne 26. března 2019, UOOU-07399/18-61.

Přehled podkladů:

Protokol o kontrole se opírá o následující podklady, které byly pořízeny v průběhu kontroly, popř. o dokumenty a skutečnosti, které jsou kontrolnímu orgánu známy z jeho úřední činnosti:

1. Kontrolní plán Úřadu pro rok 2018, č.j. UOOU-07399/18-1;
2. Analýza před zahájením kontroly ze dne 9. července 2018, č.j. UOOU-07399/18-2:
3. Vložení dokumentu ze dne 9. července 2018 – XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, XXXXXXXXXXXXXX
4. Oznámení o zahájení kontroly ze dne 20. července 2018, č.j. UOOU-07399/18-4;
5. Sdělení SÚKL - informace a dokumentace od SÚKL ze dne 27. srpna 2018, č.j. UOOU07399/18-5 + přílohy:

- Pověření Ing. Zdeňka Kusovského, MBA ze dne 8. srpna 2018
- Písemná zpráva o provozu CÚeR

- Informace o zabezpečení osobních údajů
- Přehled přístupových účtů
- Opatreni_incident_CUER
- Bezpečnostni Testy (3x)
- Příkaz ředitele SÚKL 787/2018 Bezpečnostní politika
- Vnitřní směrnice XXXX Ochrana osobních údajů v SÚKL
- Vnitřní směrnice XXXXXXXXX Politika v oblasti bezpečnosti informací
- Formulář žádosti o stanovisko Hlavního architekta eGovernmentu k plánovanému ICT projektu – typ A (duben 2016)
- Stanovisko odboru Hlavního architekta eGovernmentu k projektu „Informační systém eRecept“
- XXXXXXXXXX Smlouva + Příloha č.1 + a Příloha č. 1A + Dodatek č. 1 a 2
- XXXXXXXXX_Smlouva_Servis + Dodatek č. 1 a 2
- Ukázky logu (XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX);

6. Žádost o součinnost k SÚKL ze dne 15. října 2018, č.j. UOOU-07399/18-6;
7. Úřední záznam – vložení dokumentu do spisu ze dne 17. října 2018, XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX;
8. Žádost SÚKL o změnu termínu ústního jednání a místního šetření ze dne 18. října 2018, č.j. UOOU-07399/18-8;
9. Odpověď Úřadu na žádost SÚKL o změnu termínu ústního jednání a místního šetření ze dne 18. října 2018, č.j. UOOU-07399/18-9;
10. Opakované sdělení SÚKL - změna termínu ústního jednání a místního šetření ze dne 19. října 2018, č.j. UOOU-07399/18-10;
11. Úřední záznam – vložení dokumentu do spisu ze dne 6. listopadu 2018, č.j. UOOU07399/18-11 – výtisk z www.sukl.cz – SÚKL je připraven plnit požadavky GDPR;
12. Úřední záznam – vložení dokumentů do spisu ze dne 6. listopadu 2018, č.j. UOOU07399/18-12 – výtisk z www.sukl.cz - kontakty na pověřence;
13. Sdělení SÚKL – kopie hlášení incidentu ze dne 25. 10. 2018 a ohlášení incidentu stejné povahy ze dne 9. listopadu 2018, č.j. UOOU-07399/18-13, dne 9. listopadu 2018 (email);
14. Sdělení SÚKL – kopie hlášení incidentu ze dne 9. listopadu 2018, č.j. UOOU-07399/1814, informace o doručení k Úřadu (e-mail);

15. Sdělení SÚKL – kopie hlášení incidentu ze dne 25. 10. 2018 č.j. UOOU-07399/18-15, dne 9. listopadu 2018 (e-mail);
16. Sdělení SÚKL – ze dne 9. listopadu 2018, č.j. UOOU-07399/18-16 – čísla jednací incidentů ze dne 25. 10. 2018 a 8. 11. 2018;
17. Návrh úředního záznamu z ústního jednání a místního šetření ze dne 8. 11. 2018, č.j. UOOU-07399/18-17;
18. Průvodní dopis k návrhu úředního záznamu ze dne 13. listopadu 2018, č.j. UOOU07399/18-18;
19. Vyjádření SÚKL k návrhu úředního záznamu, č.j. UOOU-07399/18-19 ze dne 14. listopadu 2018;
20. Sdělení SÚKL k návrhu úředního záznamu, č.j. UOOU-07399/18-20 ze dne 14. listopadu 2018;
21. Úřední záznam o telefonickém hovoru ze dne 15. listopadu 2018, č.j. UOOU07399/18-21;
22. Sdělení SÚKL, č.j. UOOU-07399/18-22, ze dne 15. listopadu 2018 + přílohy:

- Kopie oznámení o bezpečnostním incidentu zaslaném Úřadu (ze dne 25. 10. 2018)
- Data logu aplikace – excelový soubor
- Písemná zpráva o provedeném auditu u poskytovatele služeb XXXXXXXXXX
- Písemná informace o provedení bezpečnostního penetračního testu CÚer ze strany NÚKIB
- XXXXXXXXXXXXXXXXX – informace
- Protokoly o likvidaci dat na přenosných médiích
- Kopie oznámení dalšího bezpečnostního incidentu
- Záznam o projednání incidentu 081109 s osobou, která jej umožnila
- Dopis provozovateli lékáren, který těžil z incidentů zneužití přístupů k CÚeR
- Printscreen z kontroly mimo transakční logy ve smyslu čl. 6.1.3 směrnice XXXXXXX
- Mailová komunikace s Úřadem ve věci konzultací přípravy na Nařízení GDPR
- Kopie datovou schránkou zaslaného dotazu Úřadu ve věci Používání telefonní informační linky;

23. Žádost o konzultaci SÚKL ze dne 20. listopadu 2018, č.j. UOOU-07399/18-23;
24. Odpověď na žádost o konzultaci ze dne 20. listopadu 2018, č.j. UOOU-07399/18-24;

25. Žádost o předání podkladů (JUDr. Žůrek) ze dne 20. listopadu 2018, č.j. UOOU07399/18-25;
26. Žádost o součinnost k SÚKL – ústní jednání ze dne 20. listopadu 2018, č.j. UOOU07399/18-26;
27. Úřední záznam – tel. rozhovor ze dne 20. listopadu 2018, č.j. UOOU-07399/18-27;
28. Úřední záznam z ústního jednání a místního šetření (čistopis)ze dne 8. 11. 2018, č.j. UOOU-07399/18-28 + přílohy:

- Předávací protokol, zátěžové testy ze dne 31. 8. 2017
- Předávací protokol, bezpečností testy ze dne 4. 9. 2017
- Akceptační protokol, Akceptace cílového řešení, ze dne 3. 8. 2017
- Akceptační protokol, Akceptace díla, Podklady k akceptaci části díla, ze dne 21. 12. 2017
- 1x CD – 9 dokumentů – viz bod 5
- Bezpečnostní incident – XXXXXXXXXX – postup
- Popis procesu vyhotovování a odeslání dopisu s aktivačními údaji pro lékaře a lékárníka
- Přístupy pracovníků zdravotních pojišťoven a jejich předávání
- Závazné pokyny a pravidla pro zaměstnance vykonávající službu/práci v SÚKL – k ochraně a bezpečností informací pro využívání prostředků výpočetní techniky
- Datový soubor – žádost lékárníka o přístup k CÚ Datová Informace o členství v ČLnK
- Datový soubor – žádost lékaře o přístup k CÚ
- Datová informace o členství v ČLK
- Informace dle zákona č. 106/1999 Sb., poskytnutá SÚKL České lékařské komoře ze dne 19. 10. 2018
- Portál pro externí identity SÚKL (XXXXXXXXXXXXXXXXXXXXXXXXXXXXX) – viz bod 2
- fotodokumentace – 5 snímků;

29. Průvodní dopis k úřednímu záznamu z ústního jednání ze dne 20. listopadu 2018, č.j. UOOU-07399/18-29;
30. Žádost o poskytnutí součinnosti NÚKIB ze dne 20. listopadu 2018, č.j. UOOU07399/18-30;
31. Opakovaná žádost o předání podkladů (JUDr. Žůrek) ze dne 6. prosince 2018, č.j. UOOU-07399/18-31;
32. Sdělení SÚKL – vyžádané informace a dokumenty ze dne 7. prosince 2018, č.j. UOOU07399/18-32 + přílohy:

- Popis identifikace incidentu „XXXXXXXXX“ včetně výčtu přístupů k CÚeR
- Výpis z databáze registru rizik vztažených k CÚeR

Žádost o povolení přístupu administrátorů poskytovatele služeb k prostředí CÚeR

- Plán auditů (kontrol) SÚKL na rok 2018 (eRecept audit 13/2018)
- Zpráva z interního auditu oddělení eRecept
- Vzory ticketů (písemných požadavků XXXXXXXX) ke zjištění informací, či údajů v CÚeR;

33. Průvodní dopis k SÚKL – zaslání úředního záznamu ze dne 7. prosince 2018, č.j. UOOU-07399/18-33;
34. Sdělení SÚKL k úřednímu záznamu ze dne 109. prosince 2018, č.j. UOOU-07399/1834;
35. Úřední záznam o provedení kontrolního úkonu ze dne 10. prosince 2018, č.j. UOOU07399/18-35;
36. Odpověď na žádost o poskytnutí součinnosti od NÚKIB ze dne 6. prosince 2018, č.j. UOOU-07399/18-36 (Úřad obdržel dne 10. prosince 2018);
37. Úřední záznam – vložení hlášení incidentu ze dne 11. prosince 2018. č.j. UOOU07399/18-37 + přílohy:

- Kopie interní sdělení (vyjádření k žádosti)
- Interní sdělení – předání spisů
- Kopie hlášení SÚKL (incident)
- Kopie vyjádření SÚKL (využití QR kódu v rámci eReceptu)
- Kopie hlášení SÚKL (incident)
- Kopie hlášení SÚKL (incident);

38. Interní sdělení – reakce na vyjádření OKA ze dne 20. prosince 2018, č.j. UOOU07399/18-38;
39. Sdělení SÚKL – doplnění ze dne 7. ledna 2018, č.j. UOOU-07399/18-39 + přílohy:

- Printscreen obrazovky mobilní aplikace XXXXXXXXXXXX zobrazující, jaké údaje byly aplikací zobrazovány
- Další komunikace mezi společností XXXXXXXXXXXXXX – dopis člena představenstva XXXXXXXXXXXXXX
- Odpověď SÚKL na předchozí zmíněný dopis XXXXXXXXXXX;

40. Žádost o součinnost k Policejnímu prezidiu ČR ze dne 9. ledna 2019, č.j. UOOU07399/18-40;
41. Žádost o součinnost k XXXXXXXXXXXX ze dne 11. ledna 2019, č.j. UOOU07399/18-41;
42. Žádost o součinnost k XXXXXXXXXXXXXXXXXXXXXXXXX ze dne 11. ledna 2019, č.j. UOOU-07399/18-42;

43. Úřední záznam – vložení dokumentu do spisu ze dne 11. ledna 2019, č.j. UOOU07399/18-43;
44. Informace pro SÚKL ze dne 11. ledna 2019, č.j. UOOU-07399/18-44;
45. Sdělení Policejní prezidium ČR ze dne 21. ledna 2019, č.j. UOOU-07399/18-45;
46. Úřední záznam z jednání v XXXXXXXXXXXXXXX ze dne 23. ledna 2019, č.j. UOOU07399/18-46;
47. Průvodní dopis ÚZ z ústního jednání XXXXXXXXXXXXXXX ze dne 23. ledna 2019, č.j. UOOU-07399/18-47;
48. Průvodní dopis ÚZ z ústního jednání k SÚKL ze dne 23. ledna 2019, č.j. UOOU07399/18-48;
49. Sdělení SÚKL k ÚZ z ústního jednání ze dne 24. ledna 2019, č.j. UOOU-07399/18-49;
50. Připomínky SÚKL k šetření v XXXXXXXXXXXXXXXXX ze dne 25. ledna 2019, č.j. UOOU07399/18-50;
51. Doplnění vyjádření k RLPO od Policejního prezidia ČR ze dne 5. února 2019, č.j. UOOU-07399/18-51;
52. XXXXXXXXXXXXXXXXXXXXXXXX – prezentace využívání eReceptů ze dne 7. 2. 2019, č.j. UOOU-07399/18-52;
53. Úřední záznam – vložení dokumentu do spisu (Dávkové rozhraní IS eRecept verze 201704B.docx), ze dne 7. února 2019, č.j. UOOU-07399/18-53;
54. Úřední záznam z ústního jednání a místního šetření v XXXXXXXXXX ze dne 6. února 2019, č.j. UOOU-07399/18-54;
55. Úřední záznam z ústního jednání a místního šetření ze dne 6. února 2019, zaslání k SÚKL ze dne 11. února 2019, č.j. UOOU-07399/18-55;
56. Úřední záznam z ústního jednání a místního šetření ze dne 6. února 2019, zaslání k XXXXXXX, ze dne 11. února 2019, č.j. UOOU-07399/18-56;
57. Sdělení XXXXXXXXX k úřednímu záznamu ze dne 12. února 2019, č.j. UOOU-07399/1856;
58. Úřední záznam ze dne 14. února 2019 – výtisk z webových stránek SÚKL „Jak správně zacházet se svými přidělenými přístupovými údaji k informačnímu systému eRecept?“, č.j. UOOU-07399/18-58;
59. Žádost o součinnost k SÚKL ze dne 15. února 2019, č.j. UOOU-07399/18-59;
60. Sdělení SÚKL ze dne 22. února 2019, č.j. UOOU-07399/18-60 + přílohy:

- Protokol o kontrole ze dne 28. 11. 2018 (XXXXXX XXXXXXXXXXXXXXXXXX)
- Bezpečnostní dokumentace dle čl. 3.1.7 Přílohy č. 1 Smlouvy o dílo;
- Standardní předpis XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX. Úřední záznam – vložení dokumentů do spisové dokumentace, ze dne 26. března 2019, UOOU-07399/18-61.

I. Průběh kontroly

1.

Důvod kontroly:

Kontrola byla zahájena na základě Kontrolního plánu Úřadu pro rok 2018, a to v návaznosti na zavedení povinnosti vydávat elektronické recepty (od 1. ledna 2018), a s tím související rozsáhlé zpracování osobních údajů v Centrálním úložišti elektronických receptů, vedeného podle § 81 zákona č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech), bylo navrženo provést kontrolu zaměřenou na zabezpečení osobních údajů při tomto zpracování.

2.

Analýza před zahájením kontroly

Ústav je organizační složkou státu, (Statut SÚKL ze dne 6. 8. 2013), Ústav je zřízen jako správní úřad zákonem č. 79/1997 Sb., o léčivech a o změnách a doplnění některých souvisejících zákonů. Pravomoc a působnost je Ústavu svěřena ustanovením § 13 odst. 1 zákona č. 378/2007 Sb., o léčivech a o změnách a doplnění některých souvisejících zákonů, v platném znění (dále také „zákon č. 378/2007 Sb.“) – „Státní ústav pro kontrolu léčiv se sídlem v Praze (dále jen „Ústav“) je správním úřadem s celostátní působností podřízeným Ministerstvu zdravotnictví“.
V rámci analýzy byla shromážděna veškerá dokumentace z úkonů Úřadu a navazujících řízení se SÚKL, a dále podněty a stížnosti, které Úřad na provoz Centrálního úložiště elektronických receptů obdržel.

Z analýzy před zahájením kontroly vyplývá, že SÚKL v rámci přípravy projektu eRecept podal k Úřadu žádost o konzultaci č.j. UOOU-11904/17 ze dne 5. listopadu 2017 – žádost SÚKL – praktiky osob, které lékařům slibují zajištění připojení k CÚeR a vyžadují k tomu osobní údaje lékařů, Úřad zaslal následně k SÚKL odpověď č.j. UOOU-11904/17-2 ze dne 1. února 2018 – doporučení obrátit se ohledně uvedeného jednání na Polici ČR.

Dne 22. prosince 2017 byla na základě obdrženého podnětu zaslána Výzva k SÚKL č.j. UOOU10756/17-4 – „zpracování OÚ lékaře v rozsahu nezbytném pro zřízení přístupu do CÚER lze jako nezbytné pro dodržení právní povinnosti provádět bez souhlasu subjektu údajů, *v* souladu s § 5 odst. 2 písm. a) zákona č. 101/2000 Sb., vyžadování souhlasu pro uvedené účely je nadbytečné a zavádějící (viz stanovisko Úřadu č. 3/2014), rodná čísla lze využívat jen *v* případech stanovených v § 13c odst. 1 zákona č. 133/2000 Sb., o evidenci obyvatel a rodných čísel, ve znění pozdějších předpisů:

a) *Jde*-li o činnost ministerstev, jiných správních úřadů, orgánů pověřených výkonem státní správy, soudů, vyplývající z jejich zákonem stanovené působnosti, nebo notářů pro potřeby vedení Centrální evidence závětí
b) stanoví-li tak zvláštní zákon
c) Se souhlasem nositele rodného čísla nebo jeho zákonného zástupce.

V uvedeném případě, výkonu státní správy, není souhlas aplikovatelný, ale v případě využití rodných čísel jde o jejich využívání podle písm. a) citovaného ustanovení. Pokud jde o *zpra*cování OÚ, měl by to SUKL při podání formuláře lékařům náležitě vysvětlit podle § 11 odst. 1 a 2 zákona č. 101/2000 Sb. Formulář SÚKL není v *tomto ohledu v souladu se* zákonem*".*
Úřad následně obdržel sdělení SÚKL ze dne 9. ledna 2018 s tím, že v uvedené věci došlo k nápravě.

3.

Zahájení kontroly

Úřad na základě pravomoci vyplývající z § 2 odst. 2 a 3, § 29 odst. 1 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů a oprávnění vyplývajícího z čl. 58 odst. 1 písm. b) Nařízení (EU) 2016/679. (dále jen „Nařízení"), zahájil dne 30. července 2018 kontrolu SÚKL zasláním Oznámení o zahájení kontroly č.j. UOOU-07399/18-4.

4.

Součinnost SÚKL a ostatních subjektů v rámci kontroly

Informace a dokumenty vyžádané v rámci Oznámení o zahájení kontroly ze dne 30. července 2018, předložil SÚKL Úřadu dne 27. srpna 2018, č.j. UOOU-07399/18-5, včetně příloh, které jsou uvedeny bod bodem 5 Přehledu podkladů tohoto protokolu o kontrole.

Dne 15. října 2018 zaslal Úřad k SÚKL přípis Žádost o součinnost, č.j. UOOU-07399/18-6. v rámci uvedené žádosti byly vyžádány doplňující informace a dokumenty

Ústní jednání a místní šetření v SÚKL proběhlo dne 8. listopadu 2018, viz Záznam z ústního jednání a místního šetření ze dne 8. listopadu 2018, č.j. UOOU.07399/18-28.

Dne 22. listopadu 2018 proběhlo ústní jednání s pověřencem pro ochranu osobních údajů SÚKL v prostorách Úřadu – viz záznam z ústního jednání ze dne 22. 11. 2018 č.j. UOOU07399/18-33.

Dne 7. prosince 2018 zaslal SÚKL k Úřadu část informací a dokumentů, které byly vyžádány při ústním jednání a místním šetření dne 22. listopadu 2018, č.j. UOOU-07399/18-32.

Dne 7. ledna 2019 zaslal SÚKL k Úřadu doplnění informací, č.j. UOOU-07399/18-40.

Dne 22. ledna 2019 proběhlo ústní jednání a místní šetření ve společnosti XXXXXXXXXXXXXXX za účasti pověřence pro ochranu osobních údajů SÚKL, viz Úřední záznam z ústního jednání a místního šetření ze dne 22. ledna 2019 v XXXXXXXXXXXXXXXX ze dne 23. února 2019, č.j. UOOU-07399/18-46.

Dne 6. února 2019 proběhlo ústní jednání a místní šetření ve XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, viz Úřední záznam z ústního jednání a místního šetření ze ne 6. února 2019, ze dne 11. února 2019, č.j. UOOU-07399/18-54.

Dne 22. února 2019 zaslal SÚKL k Úřadu informace a dokumenty (č.j. uoou-07399/18-60) vyžádané v rámci Žádosti o součinnost k SÚKL ze dne 15. února 2019, č.j. UOOU-07399/18-59.

II. Zjištěný skutkový stav

Postavení SÚKL (dále také „Ústav“) **a Centrálního úložiště elektronických receptů**

Ve smyslu § 13 odst. 1 zákona č. 378/2007 Sb. o léčivech „Státní ústav pro kontrolu léčiv se sídlem v Praze (dále také „Ústav“) je správním úřadem s celostátní působností podřízeným Ministerstvu zdravotnictví“. Ve smyslu § 13 odst. 2 písm. n) uvedeného zákona Ústav „spravuje registr léčivých přípravků s omezením“.

Ve smyslu § 13 odst. 3 písm. n) zákona č. 378/2007 Sb. *v* oblasti humánních léčiv., Ústav v oblasti humánních léčiv „zřizuje a provozuje centrální datové úložiště pro sběr a zpracování elektronicky předepisovaných léčivých přípravků“.

Ve smyslu § 81 odst. 1 písm. a) – g) zákona č. 378/2007 Sb. „Centrální úložiště elektronických receptů zřizuje Ústav jako svou organizační součást k zabezpečení plnění těchto úkolů:

a) přijímat a shromažďovat elektronické recepty zaslané předepisujícími lékaři,
b) sdělit lékaři bezprostředně po obdržení elektronického receptu jeho identifikační znak, na jehož základě bude předepsaný léčivý přípravek vydán v lékárně,
c) zpřístupnit bezúplatně elektronický recept, na němž předepsaný léčivý přípravek má být vydán, farmaceutovi vydávajícímu v příslušné lékárně léčivé přípravky, a to bezprostředně po obdržení jeho žádosti,
d) zabezpečit bezúplatně nepřetržitý přístup do databáze elektronických receptů *p*ředepisujícím lékařům a farmaceutům vydávajícím v lékárnách předepsané léčivé přípravky; rovněž zabezpečit bezúplatně přístup do databáze elektronických receptů zdravotním pojišťovnám za účelem provádění kontrolní činnosti podle zákona upravujícího veřejné zdravotní pojištění,
e) zajistit ochranu a bezpečnost v databázi uložených elektronických receptů před jejich poškozením, zneužitím nebo ztrátou podle zvláštního právního předpisu, f) zajistit ochranu a předání údajů v případě ukončení činnosti,
*g) neo*dkladně označit elektronický recept zpřístupněný podle písmene c) a vydaný podle § 82“.

Ve smyslu § 81 odst. 2 zákona č. 378/2007 Sb. „Centrální úložiště elektronických receptů je propojeno s registrem pro léčivé přípravky s omezením podle § 81a za účelem zajištění dodržování omezení stanoveného v rozhodnutí o registraci podle § 39 odst. 4 písm. c) a

omezení stanoveného prováděcím právním předpisem u individuálně připravovaného léčivého přípravku s obsahem konopí pro léčebné použití“.

Důvodová zpráva k tomuto zákonu obsahuje sdělení, že „*v* důsledku nových činností zavedených předpisy Společenství je činnost Ústavu rozšířena o odpovědnosti v *oblasti* hemovigilance (sledování závažných nežádoucích reakcí a událostí) a *povinnost poskytovat* Komisi zprávu o závažných nežádoucích událostech a reakcích.

*D*ále, že ve zvýšené míře se klade důraz na sledování bezpečnosti léčivých přípravků při jejich praktickém používání a vytvářejí se podmínky pro aktivní přístup regulačních institucí ke shromažďování a získávání potřebných údajů o bezpečnosti léčiv a zlepšuje se dostupnost údajů z různých zdrojů a databází pro tyto účely. V návrhu zákona v zájmu zajištění maximální dostupnosti léčiv občanům při zachování záruk za odpovídající vlastnosti *a* informace poskytované k *jednotl*ivým léčivým přípravkům se upřesňuje odpovědnost jednotlivých správních úřadů a provozovatelů“.

V návrhu zákona je zároveň sledován cíl, aby každý regulační prvek, včetně povinností a omezení uplatňovaných vůči soukromoprávním subjektům, byl opodstatněn přínosem pro ochranu zdraví veřejnosti a v případě veterinárních léčivých přípravků dále přínosem v oblasti ochrany a tvorby zdraví a pohody zvířat a ochrany životního prostředí, zejména s ohledem na dostupnost léčiv, jejich odpovídající vlastnosti a způsob používání. Cílem návrhu zákona je dále vytvořit podmínky pro důsledné vymáhání práva v příslušných oblastech při zohlednění dosavadních zkušeností a odstranit nejasnosti a hraniční situace a zajistit tak zvyšování právních jistot dotčených subjektů, a to zejména pokud jde o ochranu veřejného zdraví či zdraví a pohody zvířat a ochranu životního prostředí před nepříznivým působením léčivých přípravků.

Architektura a provoz CÚeR se dále odvíjí od:

Vyhlášky č. 415/2017 Sb., k provedení některých ustanovení zákona o léčivech týkající se elektronických receptů; Vyhlášky č. 84/2008 Sb., o správné lékárenské praxi, bližších podmínkách zacházení s léčivy v lékárnách, zdravotnických zařízeních a u dalších provozovatelů a zařízení vydávajících léčivé přípravky; Vyhlášky č. 54/2008 Sb., o způsobu předepisování léčivých přípravků, údajích uváděných na lékařském předpisu a o pravidlech používání lékařských předpisů; Vyhlášky č. 236/2015 Sb., kterou se stanovují podmínky pro předepisování, přípravu, výdej a používání individuálně připravovaných léčivých přípravků s obsahem konopí pro léčebné použití; zákona č. 167/1998 Sb., o návykových látkách, ve znění pozdějších předpisů; zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování /zákon o zdravotních službách), ve znění pozdějších předpisů; zákona č. 48/1997 Sb., o veřejném zdravotním pojištění, ve znění pozdějších předpisů; zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů - od 25. 5. 2018 Nařízení (EU) 2016; zákona č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů; zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů;

zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně dalších zákonů, ve znění pozdějších předpisů; zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů, zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů; vyhlášky 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).

III. Porovnání zjištěného skutkového stavu s platnou právní úpravou

Kontrolní zjištění č. 1

Dle čl. 4 odst. 1 Nařízení se "osobními údaji" rozumí veškeré informace o 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.“
Dle čl. 4 odst. 15 Nařízení se rozumí „údaji o zdravotním stavu“ osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním sta*vu.*
Dle čl. 9 odst. 2 písm. i) Nařízení „zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků, na základě práva Unie nebo členského státu, které stanoví odpovídající a zvláštní opatření pro zajištění práv a svobod subjektu údajů, zejména služebního tajemství.“

eRecept a zadávání informací do CÚeR:

eRecept je recept vystavený v elektronické podobě. Lékařem vystavený eRecept je uložen do tzv. Centrálního úložiště elektronických receptů. Každému receptu je přidělen unikátní identifikátor. V lékárně pak lékárník načte identifikátor eReceptu a pokud je eRecept v CÚeR nalezen, vydá předepsaný léčivý přípravek pacientovi. Informace o výdeji se zapíše do CÚeR.

Hlavní zdroj údajů pro systém eRecept tvoří elektronický recept vytvořený lékařem. Lékař prostřednictvím jednoho ze způsobu komunikace (ambulantní/nemocniční systém) zasílá identifikační údaje pacienta společně s dalšími údaji, které jsou nezbytné pro elektronickou preskripci, do systému eRecept, čímž dochází k vytvoření elektronického receptu v systému eRecept.

Dalším zdrojem údajů je pak provedení záznamu o výdeji lékárníkem, při kterém je k elektronickému receptu doplněn a zaslán do systému eRecept jeho výdej, který obsahuje další údaje, zejména o vydávajícím lékárníkovi a rovněž vydaných léčivých přípravcích (vzhledem k možnosti substituce mohou být odlišné od předepsaných).

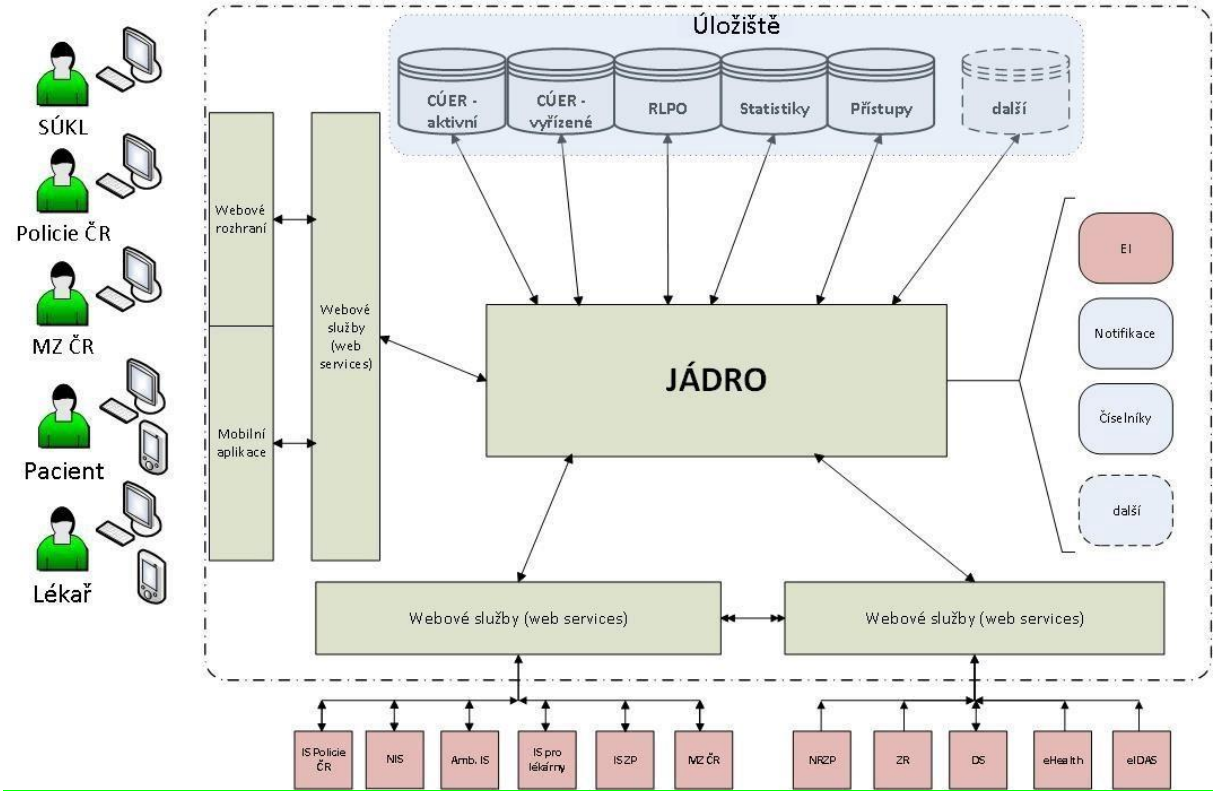
Systém eRecept obsahuje osobní údaje několika kategorií subjektů údajů, přičemž celkový objem subjektů údajů, jejichž osobní údaje jsou v systému eRecept zpracovávány, dle jednotlivých kategorií je následující: cca 10,5 miliónů pacientů v cílovém stavu cca 47 tisíc lékařů (vč. zubních lékařů) cca 11 tisíc lékárníků.

Přílohou tohoto protokolu o kontrole je tabulka s rozsahem evidovaných dat, kterou v rámci kontroly předložila Kontrolovaná osoba (příloha č.j. UOOU-07399/18-5 ze dne 27. srpna 2018), kde jsou zobrazeny všechny atributy evidované v systému eRecept (XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX).

IS eRecept (schéma a architektura CÚeR)

IS eRecept (dále také „Systém“) zahrnuje CÚeR dle § 81 zákona o léčivech, registr pro léčivé přípravky s omezením dle § 81a zákona o léčivech a další komponenty (viz Smlouva o dílo uzavřená mezi SÚKL a XXXXXXXXXXXXXXXXXXX).

Schéma a architektura Centrálního úložiště elektronických receptů, viz Příloha č. 1 – Specifikace předmětu díla - Smlouva o dílo uzavřená mezi SÚKL a XXXXXXXXXXXXXXXXXXXXXXXX, příloha č.j. UOOU-07399/18-5 ze dne 28. srpna 2018 – CD, dále str. 39-44 tohoto protokolu o kontrole.



Z Přílohy č. 1 čl. 1.3 Databáze vyplývá, že Informační systém e-Recept bude využívat k ukládání dat databázi XXXXXXXXXXXXXX.

Data budou ukládána do více databází, přičemž hlavními jsou:
CÚeR – aktivní recepty; CÚeR – vyřízené recepty; Registr pro léčivé přípravky s omezením (RLPO); Statistická data; Přístupy (primárně bude sloužit jako zdroj požadovaných informací pro bezpečnostní složky, případně pro Polici ČR).

Jednotlivé subjekty, které mohou osobní údaje zpracovávané v CÚeR využívat, tak činí pouze omezeně za konkrétně vymezeným účelem a pomocí přesně definovaného procesu.

Role pacientů, lékařů, lékárníků, zdravotních pojišťoven, Policie ČR a Ministerstva zdravotnictví ČR

Pacient

Kontrolou bylo zjištěno, že k jednoznačnému přiřazení konkrétního eReceptu konkrétnímu člověku je nutné ztotožnění pacienta tak, aby se stoprocentně zamezilo tomu, že by někdo omylem mohl vidět i cizí recepty s předepsanými léky, jedná se o vysokou ochranu osobních údajů každého pacienta. Pokud k takovému jednoznačnému přiřazení nedojde a eRecept je přesto vystaven, zůstane v jakémsi společném „zásobníku“, kde jsou všechny eRecepty neztotožněných pacientů. K těmto eReceptům je následně přístup pouze podle identifikátoru (tedy ten, kdo se chce na daný eRecept podívat, musí znát jeho identifikátor).

Ale tyto eRecepty nejsou zobrazovány v tzv. lékovém záznamu pacienta.
Pro potřebu vytváření elektronického lékového záznamu pacienta je nutné ztotožnění pacienta v Registru obyvatel (ROB) při založení eReceptu lékařem.

Postup při ztotožnění pacienta:

XXXX

XXXX

Ve webové aplikaci ke svému účtu, který je veden v systému eRecept, si nastaví heslo a uvede identifikátor mobilního zařízení, na kterém se bude chtít do mobilní aplikace přihlásit (např. IMEI). Při přihlášení v mobilní aplikaci uživatel uvede své uživatelské jméno (přidělené systémem eRecept) a heslo. Systém ověří, zda se uživatel přihlašuje na mobilním zařízení s identifikátorem mobilního zařízení uvedeného u účtu pacienta, ověří uživatelské jméno a heslo. V případě úspěšného ověření je pacient do aplikace úspěšně přihlášen.

Postup pro registraci a aktivaci uživatelského profilu – viz příloha č. 16 Analýzy před zahájením kontroly, č.j. uoou-07399/18-2 ze dne 9. července 2018.

Pacient se v rámci tohoto procesu může přihlásit do systému eRecept, aby mohl prohlížet své eRecepty.

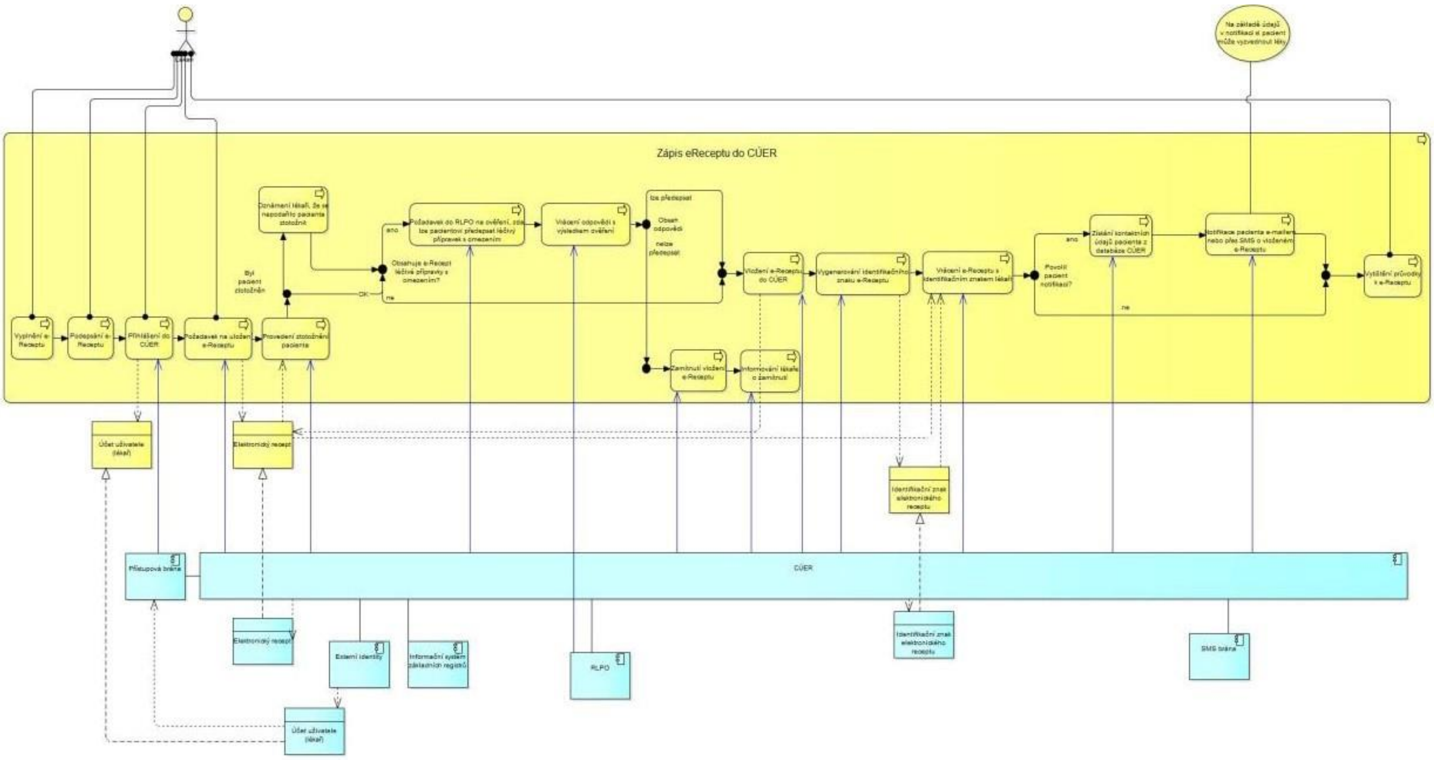
Popis procesu detailně popsán v písemné zprávě o provozu CÚeR – příloha č.j. UOOU07399/18-5 ze dne 27. srpna 2018 – popsán proces, jakým způsobem dochází k autentizaci pacienta do systému CÚeR a k vyhledání jeho receptů a jejich prohlížení.

Lékař

Ve smyslu § 81 odst. 1 písm. d) zákona č. 378/2007 Sb., je SÚKL prostřednictvím Centrálního úložiště elektronických receptů povinen zabezpečit bezúplatně nepřetržitý přístup do databáze receptů předepisujícím lékařům a farmaceutům vydávajícím v lékárnách předepsané léčivé přípravky.
Lékař má možnost vidět všechny recepty, které vystavil nebo recept, ke kterému zná identifikátor receptu. Lékař má možnost vidět výdeje u receptů, které sám vystavil. K zobrazení dat používá lékař webovou, mobilní aplikaci nebo svoji aplikaci, která komunikuje s CÚeR.
XXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXX.

Lékař předepisuje pro pacienta eRecept, ve většině případů předepisuje eRecept prostřednictvím svého systému (ambulantní/nemocniční systém).



V tomto procesu provádí lékař zápis elektronického receptu do systému eRecept. Přihlášení může probíhat třemi způsoby:

1. Prostřednictvím lékařského SW a webových služeb
2. Prostřednictvím mobilní aplikace (jako první krok před vyplněním eReceptu)
3. Prostřednictvím webové aplikace (jako první krok před vyplněním eReceptu)

Rozsah údajů evidovaných lékařem na eReceptu:

Osobní údaje pacienta (nejsou všechny povinné): číslo dokladu; druh dokladu; číslo pojištěnce; datum narození; jméno; příjmení; pohlaví; hmotnost; email; telefon; zdravotní pojišťovna; druh pojištění; adresa pacienta (ulice, číslo popisné, číslo orientační, číslo evidenční, obec, část obce, okres, PSČ, název věznice pacienta).
Údaje o předepisujícím lékaři: jméno; příjmení; odbornost; oddělení; kód pracoviště; telefon; IČZ; IČP.

Údaje o doporučujícím lékaři: jméno; příjmení, odbornost; název poskytovatele telefon; IČZ; IČP, IČ poskytovatele; DIČ poskytovatele.
Údaje o léčivém přípravku: název léčivého přípravku (HVLP – hromadně vyráběný léčivý přípravek, neregHVLP – neregistrovaný; hromadně vyráběný léčivý přípravek, IPLP-individuálně připravovaný léčivý přípravek, INN-mezinárodní nechráněný název); léková forma (HVLP, neregHVLP, INN); velikost balení (HVLP, neregHVLP, INN); síla (HVLP, neregHVLP, INN), cesta podání (HVLP, neregHVLP, INN), ATC skupina (HVLP, neregHVLP); kód SUKL (HVLP); Množství (HVLP, neregHVLP, INN); úhrada – zda se hradí ze zdravotního pojištění (HVLP, neregHVLP, INN); diagnóza (HVLP, neregHVLP, INN); přidružená diagnóza (HVLP, neregHVLP, INN), symboly (HVLP, neregHVLP, INN); číslo žádanky (HVLP, neregHVLP, INN); návod (HVLP, neregHVLP, INN), postup přípravy (IPLP); složka – surovina, z které se IPLP realizuje (IPLP).

Provádění změn údajů eReceptu v CÚER - tento proces přistupuje k osobním údajům pacienta.
Aktér: lékař, který mění eRecept pro pacienta, který byl vydaný daným lékařem.

Storno eReceptu - tento proces přistupuje k osobním údajům pacienta.
Aktér: lékař, který jeho předepsaný eRecept stornuje.
Zobrazení provedených výdejů k eReceptu - tento proces přistupuje k osobním údajům pacienta.
Aktér: lékař, který zobrazuje provedené výdeje k jeho vystaveným eReceptům.

Lékař má možnost si z CÚeR stáhnout provedené výdeje včetně vydaných léčivých přípravků ke svým vydaným receptům.
Rozsah poskytnutých dat lékaři při zobrazení výdeje: základní informace o výdeji: identifikátor výdeje; datum výdeje; poznámka lékárníka.
Vydaný léčivý přípravek: množství; název; síla; forma; balení; doba použitelnosti; návod.
Informace o vydávajícím: název poskytovatele; telefon; adresa poskytovatele; ICŽ poskytovatele; kód pracoviště.

Načtení eReceptu z CÚeR na základě identifikátoru eReceptu (který získal lékař od pacienta) - tento proces přistupuje k osobním údajům pacienta.

Popis procesu detailně popsán v písemné zprávě o provozu CÚeR – příloha č.j. UOOU07399/18-5 ze dne 27. srpna 2018.

Lékárník

Ve smyslu § 81 odst. 1 písm. d) zákona č. 378/2007 Sb., je SÚKL prostřednictvím Centrálního úložiště elektronických receptů povinen *zabe*zpečit bezúplatně nepřetržitý přístup do databáze receptů předepisujícím lékařům a farmaceutům vydávajícím v lékárnách předepsané léčivé přípravky.

Lékárník má přístup ke všem receptům, které jsou v CÚeR. Lékárník může načíst jakýkoliv recept, pokud zná jeho identifikátor.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXX.

Načtení eReceptu lékárníkem z CÚeR - tento proces přistupuje k osobním údajům pacienta. Aktér: lékárník, který načítá eRecept z CÚeR, aby na něj mohl následně provést např. výdej. V tomto procesu provádí lékárník načtení eReceptu ze systému CÚeR na základě identifikátoru eReceptu, který získal od pacienta.

Zápis záznamu o výdeji léků do CÚeR: tento proces přistupuje k osobním údajům pacienta. Aktér: lékárník, který na daný e Recept provádí výdej léčivých přípravků.

Změna záznamu o výdeji v CÚeR: tento proces přistupuje k osobním údajům pacienta.

Storno záznamu o výdeji v CÚeR: tento proces přistupuje k osobním údajům pacienta.

Zápis záznamu o výdeji či přípravě léčivého přípravku s omezením bez předpisu: tento proces přistupuje k osobním údajům pacienta.
Zápis záznamu o výdeji či přípravě léčivého přípravku s omezením s předpisem: tento proces přistupuje k osobním údajům pacienta.

Storno záznamu o výdeji či předpisu léčivého přípravku s omezením bez předpisu: tento proces přistupuje k osobním údajům pacienta.

Změna pojišťovny na předpisu (eReceptu): tento proces přistupuje k osobním údajům pacienta.

Popis procesu detailně popsán v písemné zprávě o provozu CÚeR – příloha č.j. UOOU07399/18-5 ze dne 27. srpna 2018.

V rámci kontroly předložila Kontrolovaná osoba kopii datového souboru žádosti lékárníka o přístup do CU a datovou informaci o členství v ČLnK; datový soubor žádosti lékaře o přístup do CU a datovou informaci o členství v ČLK a kopie Rozhodnutí o odejmutí oprávnění k poskytování zdravotních služeb a kopii Rozhodnutí o udělení oprávnění k poskytování zdravotních služeb a tomu odpovídající výpis z Portálu pro externí identity – zrušení a přidělení přístupu (příloha č.j. UOOU-07399/18-28 ze dne 20. listopadu 2018.
Dále SÚKL doložil písemnou informaci popisu procesu vyhotovování a odeslání dopisu s aktivačními údaji pro lékaře a lékárníka – příloha č.j. UOOU-07399/18-28 ze dne 20. listopadu 2018.

Kontrolou bylo zjištěno, že pravidla a postup pro manuální zpracování žádostí o přístup do Centrálního úložiště elektronických receptů či Registru pro léčivé přípravky s omezením a je určen pro pracovníky oddělení ERP (Elektronický recept) a OSS (Spisová služba) jsou stanoveny směrnicí XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX (postup pro zpracování žádostí lékařů, farmaceutů a zdravotních pojišťoven o přístup do CÚeR) - postup dle směrnic auditován – viz Zpráva z auditu ze dne 26. 11. 2018 – příloha č.j. UOOU07399/18-32 ze dne 7. prosince 2018.

Kontrolující prověřili informace podané v rámci kontroly SÚKL, a to v rámci ústního jednání a místního šetření, které se uskutečnilo ve společnosti XXXXXXXXXXXXXXX dne 22. ledna 2019 (Úřední záznam ze dne 22. ledna 2019, č.j. UOOU-07399/18-46). Ověřovány byly informace o přístupu do CÚeR jak z pohledu lékárny, tak z pohledu poskytovatele lékárenského softwaru. Postupy lékárníka při výdeji léčivého přípravku byly demonstrovány prostřednictvím testovacího/vývojového prostředí CÚeR poskytovaného SÚKL a bylo zjištěno:

- Načítá se kód receptu přes čárový kód, přes QR kód, který je vždy umístěn na receptu (bez ohledu na to, zda je vytištěn, v SMS nebo e-mailu), nebo zadáním alfanumerického řetězce na eReceptu.
- Bez kódu nelze provést výdej – načtení kódu umožňuje připojení k receptu uloženému v CÚeR – tímto dojde k propojení receptu s lékárenským systémem.
- Lékárník se autentizuje prostřednictvím XXX.
- Po načtení kódu se lékárníkovi zobrazí údaje pacienta (číslo pojištěnce/rodné číslo, léčivý přípravek, datum vydání receptu, jméno a příjmení předepisujícího lékaře – viz příloha č.j. UOOU-07399/18-46 ze dne 22. ledna 2019). Lékárenský SW propojí informaci o požadavku na léčivý přípravek s evidencí léčivých přípravků v lékárně. Po uhrazení léčivého přípravku, resp. zobrazení informace o ceně úhrady ZP, je léčivý

přípravek vydán. Informace o vydaném léčivém přípravku je uložena v CÚeR. Současně se tato informace ukládá v lékárenském SW lékárny a recept je tzv. zavřen – v demonstrovaném systému byla červenou barvou označena informace o výdeji léčivého přípravku.

- V případě, že jedním receptem jsou předepsány dva léčivé přípravky a je vydán v lékárně pouze jeden, který je v CÚeR označen jako vydaný, má přístup k receptu další lékárník, kterému je recept předložen.
- Možnost opravy údajů o výdeji léčivého přípravku (např. retaxace-přezkoušení lékařských předpisů po cenové stránce) v CÚeR má lékárna (oprávnění lékárníci), ve které byl léčivý přípravek vydán. V praxi se tak děje při každodenní kontrole vydaných léčivých přípravků. Z toho důvodu je ve statistice SÚKL přibližně dvojnásobný počet přístupů lékáren k receptu v CÚeR oproti počtu vydaných receptů lékaři.
- Obdobně postupuje lékárník při výdeje léčivého přípravku s omezením.
- Informace z lékárenského systému jsou uchovávány po dobu 5 let v lékárně, dále jsou využívány pro informace odesílané SÚKL (evidence léčiv), statistiku, skladové hospodářství a účetnictví lékárny.

Kontrolou bylo zjištěno, že prostřednictvím IS e-Recept jsou v rámci CÚeR zpracovávány osobní údaje pacienta: číslo dokladu; druh dokladu; číslo pojištěnce; datum narození; jméno; příjmení; pohlaví; hmotnost; email; telefon; zdravotní pojišťovna; druh pojištění; adresa pacienta (ulice, číslo popisné, číslo orientační, číslo evidenční, obec, část obce, okres, PSČ, název věznice pacienta); údaje o předepisujícím lékaři: jméno; příjmení; odbornost; oddělení; kód pracoviště; telefon; IČZ; IČP.
Údaje o doporučujícím lékaři: jméno; příjmení, odbornost; název poskytovatele telefon; IČZ; IČP, IČ poskytovatele; DIČ poskytovatele; údaje o vydávajícím lékárníkovi: jméno/jména, příjmení, adresa, evidenční číslo vydávajícího lékárníka.
V registru léčivých přípravků s omezením (RLPO), který je propojen s CÚeR jsou ve smyslu § 81a odst. 1 písm. b) zákona o léčivech zpracovávány údaje o poskytovatelích zdravotních služeb, kteří tyto léčivé přípravky předepsali, farmaceutech a pacientech, kterým byly tyto léčivé přípravky připraveny nebo vydány v rozsahu: identifikační číslo pojištěnce, nejde-li o pojištěnce veřejného zdravotního pojištění, jméno, příjmení a datum narození fyzické osoby, které byl léčivý přípravek vydán, a dále kód léčivého přípravku, je-li přidělen Ústavem, vydané množství, datum vystavení receptu, datum výdeje a identifikaci předepisujícího poskytovatele zdravotních služeb, uvedením jeho čísla přiděleného zdravotní pojišťovnou, bylo-li zdravotní pojišťovnou přiděleno, vydávajícího farmaceuta uvedením jeho čísla přiděleného Českou lékárnickou komorou a provozovatele oprávněného k výdeji.

Subjekty údajů, tj. pacienti, předepisující lékaři, doporučující lékaři a lékárníci, kteří léčivý přípravek na eRecept vydali, jsou v rámci CÚeR na základě zpracovávaných údajů jednoznačně identifikovatelní**, tedy Kontrolovaná osoba zpracovává údaje, které jsou osobními údaji**

uvedených subjektů údajů ve smyslu čl. 4 odst. 1 Nařízení a ve smyslu čl. 4 odst. 7 Nařízení je v postavení správce osobních údajů.

Zpracování osobních údajů je Kontrolovanou osobou jako správcem prováděno zákonně, neboť je prováděno v souladu s čl. 6 odst. 1 písm. c) Nařízení, neboť je „nezbytné pro splnění právní povinnosti, která se na správce vztahuje", dále zákonnost zpracování osobních údajů vyplývá z čl. 6 odst. 1 písm. e) Nařízení „zpracování je nezbytné pro splnění úkolu prováděném ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce", přičemž tyto povinnosti vyplývají Kontrolované osobě z ustanovení zvláštního právního předpisu členského státu Unie, kterým je zákon č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech).

Kontrolní zjištění č. 2

V rámci IS eRecept jsou v CÚeR zpracovávány další údaje o léčivém přípravku, předepsaném konkrétnímu pacientovi: název léčivého přípravku (HVLP – hromadně vyráběný léčivý přípravek, neregHVLP – neregistrovaný; hromadně vyráběný léčivý přípravek, IPLP-individuálně připravovaný léčivý přípravek, INN-mezinárodní nechráněný název); léková forma (HVLP, neregHVLP, INN); velikost balení (HVLP, neregHVLP, INN); síla (HVLP, neregHVLP, INN), cesta podání (HVLP, neregHVLP, INN), ATC skupina (HVLP, neregHVLP); kód SUKL (HVLP); Množství (HVLP, neregHVLP, INN); úhrada – zda se hradí ze zdravotního pojištění (HVLP, neregHVLP, INN); **diagnóza** (HVLP, neregHVLP, INN); **přidružená diagnóza** (HVLP, neregHVLP, INN), symboly (HVLP, neregHVLP, INN); číslo žádanky (HVLP, neregHVLP, INN); návod (HVLP, neregHVLP, INN), postup přípravy (IPLP); složka – surovina, z které se IPLP realizuje (IPLP).

eRecept uložený v CÚeR obsahuje název a kód předepsaného léčivého přípravku a diagnózu identifikovaného subjektu údajů, **tyto údaje vypovídají o zdravotním stavu subjektu údajů ve smyslu čl. 4 odst. 15 Nařízení a jsou ve smyslu čl. 9 odst. 1 Nařízení zvláštními kategoriemi osobních údajů.**

Zpracovávání zvláštních kategorií osobních údajů Kontrolovanou osobou **je zákonné, neboť probíhá na základě právního titulu vyplývajícího z čl. 9 odst. 2 písm. i**) „zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na základě práva Unie nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem a při splnění podmínek a záruk uvedených v odstavci 4"**, a čl. 9 písm. h) Nařízení** „zpracování je nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví, jako je zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků….".

Zpracování zvláštních kategorií osobních údajů probíhá v souladu s Nařízením na základě práva členského státu vyjádřeného ustanovením § 13 odst. 1 zákona č. 378/2007 Sb. o léčivech „Státní ústav pro kontrolu léčiv se sídlem v Praze (dále také „Ústav") je správním

úřadem s celostátní působností podřízeným Ministerstvu zdravotnictví“, ve smyslu § 13 odst. 2 písm. n) uvedeného zákona Ústav „spravuje registr léčivých přípravků s omezením“, dále dle § 3 písm. n) zákona č. 378/2007 Sb., Ústav „zřizuje a provozuje centrální datové úložiště pro sběr a zpracování elektronicky předepisovaných léčivých přípravků“, dále dle § 81 odst. 1 písm. a) – g) zákona č. 378/2007 Sb. „Centrální úložiště elektronických receptů zřizuje Ústav jako svou organizační součást k zabezpečení plnění těchto úkolů:

a) přijímat a shromažďovat elektronické recepty zaslané předepisujícími lékaři,
b) sdělit lékaři bezprostředně po obdržení elektronického receptu jeho identifikační znak, na jehož základě bude předepsaný léčivý přípravek vydán v lékárně,
c) zpřístupnit bezúplatně elektronický recept, na němž předepsaný léčivý přípravek má být vydán, farmaceutovi vydávajícímu v příslušné lékárně léčivé přípravky, *a to* bezprostředně po obdržení jeho žádosti,
d) zabezpečit bezúplatně nepřetržitý přístup do databáze elektronických receptů předepisujícím lékařům a farmaceutům vydávajícím v lékárnách předepsané léčivé přípravky; rovněž zabezpečit bezúplatně přístup do databáze elektronických receptů zdravotním pojišťovnám za účelem provádění kontrolní činnosti podle zákona upravujícího veřejné zdravotní pojištění,
e) zajistit ochranu a bezpečnost v databázi uložených elektronických receptů před jejich poškozením, zneužitím nebo ztrátou podle zvláštního právního předpisu, f) zajistit ochranu a předání údajů v případě ukončení činnosti,
g) neodkladně označit elektronický recept zpřístupněný podle písmene c) a vydaný podle § 82,

a § 81 odst. 2 zákona č. 378/2007 Sb. „Centrální úložiště elektronických receptů je propojeno s registrem pro léčivé přípravky s omezením podle § 81a za účelem zajištění dodržování omezení stanoveného v rozhodnutí o registraci podle § 39 odst. 4 písm. c) a omezení stanoveného prováděcím právním předpisem u individuálně připravovaného léčivého přípravku s obsahem konopí pro léčebné použití“, přičemž údaje zpracovávané v RLPO jsou vymezeny ustanovením § 81a odst. 1 písm. b) zákona č. 378/2007 Sb., o léčivech, bezúplatný nepřetržitý přístup pro předepisujícímu lékaři a vydávajícímu farmaceutovi zajistí Ústav ve smyslu § 81a odst. 1 písm. c) a d) zákona č. 378/2007 Sb.

<u>Kontrolní zjištění č. 3</u>

Archivace eReceptu je stanovena SUKL na dobu 5 let od provedení výdeje eReceptu. Po 5-ti letech je eRecept z databáze trvale odstraněn. V případě, že byl pacient ztotožněn proti Základním registrům a je tak v systému eRecept veden o pacientovi jeho záznam, je jeho záznam odstraněn s posledním odstraňovaným eReceptem.

Doba uchování 5ti let je odvozena od doby uchování receptů dle § 17 odst. 2 vyhlášky č. 84/2008 Sb., o správné lékárenské praxi a odpovídá nejkratší době uchování dle přílohy

č. 3 vyhlášky č. 98/2012 Sb., o zdravotnické dokumentaci, přičemž ustanovení § 1 a příloha č. 1 a 2 vyhlášky č. 54/2008 Sb., o způsobu předepisování léčivých přípravků, údajích uváděných na lékařském předpisu a o pravidlech používání lékařských předpisů upravuje dfc. definici receptu.

Registr léčivých přípravků s omezením – ve smyslu § 81a odst. 1 písm. e) zákona č. 378/2007 Sb. Ústav „zpracovává a uchovává osobní údaje o pacientech, o předepisujících poskytovatelích zdravotních služeb a vydávajících farmaceutech po uskutečnění výdej pouze po dobu, pro kterou je množstevní omezení léčivého přípravku stanoveno*:*

1. *v rozh*odnutí o registraci podle § 39 odst. 4 písm. c) *nebo* § 39 odst. 5 u registrovaný*ch* léčivých přípravků, nebo

2. v prováděcím právním předpise podle § 79a odst. 1 u individuálně připravovaných léčivých přípravků s obsahem konopí pro léčebné použití; v případě, že k výdeji nedošlo, počítá se lhůta od data ověření, zda jsou splněny podmínky pro přípravu“.

Doba uchování osobních údajů a zvláštních kategorií osobních údajů v CÚeR je stanovena v souladu s ustanovením čl. 5 odst. 1 písm. e) Nařízení.

Kontrolní zjištění č. 4

Dle čl. 4 odst. 7 Nařízení se "správcem" rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.

Kontrolovaná osoba je orgánem veřejné moci; účel, způsob a prostředky zpracování osobních údajů v CÚeR byly Kontrolované osobě stanoveny zvláštním právním předpisem, kterým je zákon č. č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech) a další související právní předpisy. Kontrolovaná osoba toto zpracování provádí a odpovídá za něj**, Kontrolovaná osoba je ve smyslu čl. 4 odst. 7 Nařízení správcem osobních údajů a zvláštních kategorií osobních údajů zpracovávaných v CÚeR a s ním propojeným RLPO, neboť dle § 13 odst. 3 písm. n) zákona č. 378/2007 Sb., zřídila a provozuje centrální datové úložiště pro sběr a zpracování elektronicky předepisovaných léčivých přípravků, dle podmínek upravených v § 81 a § 81a zákona č. 378/2007 Sb.**

Kontrolní zjištění č. 5

Dle čl. 4 odst. 2 Nařízení se "zpracováním" rozumí 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“.

Kontrolovaná osoba tím, že prostřednictvím IS eRecept v rámci CÚeR s nímž je ve smyslu § 81 odst. 2 zákona č. 372/2007 Sb., propojen RLPO provádí automatizované postupy, tj. shromažďuje, zaznamenává osobní údaje subjektů údajů a zvláštní kategorie osobních údajů těchto subjektů údajů, a to za účelem jejich dalšího automatizovaného zpracování, provádí ve smyslu čl. 4 odst. 2 Nařízení, zpracování osobních údajů.

Kontrolní zjištění č. 6

Zdravotní pojišťovna

Zdravotní pojišťovna má možnost získat z CÚeR všechna data (předpisy, výdeje) za její pojištěnce, ve smyslu § 81 odst. 1 písm. d) zákona č. 378/2007 Sb., SÚKL je prostřednictvím Centrálního úložiště elektronických receptů povinen „zabezpečit bezúplatně přístup do databáze elektronických receptů zdravotním pojišťovnám za účelem provádění kontrolní činnosti podle zákona upravujícího veřejné zdravotní pojištění“.

Z přílohy č. 1A Smlouvy o dílo (uzavřené se XXXXXXXXXXXXXXXXXXXX ze dne 16. prosince 2016) – Specifikace procesů (čl. 4 Zdravotní pojišťovna) čl. 4.1 Načtení eReceptu za konkrétní ZP vyplývá, že „Zdravotní pojišťovna bude mít k dispozici načtení eRp realizovaných „svými“ pojištěnci (pacienty*) za* jakékoliv období, po které budou eRp uloženy v CÚER, tedy dle skartačního řádu. Budou k dispozici přehledy vystavených a vydaných eRp, případně částečně vydaných eRp. Dále budou k dispozici přehledy vystavených, ale nevydaných eR*p,* resp. částečně nevydaných eRp. Přehledy budou vytvářeny podle různých výběrových kritérií, *v* různém členění a řazení. ZP bude moci v kombinaci těchto kritérií načíst libovolnou statistiku eRp“.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXX.

Kontrolou bylo zjištěno, že oprávnění zaměstnanců zdravotních pojišťoven přistupovat k CÚeR se zakládá na jejich pracovním poměru. Zdravotní pojišťovna podá volně formulovanou žádost o povolení přístupu pro svého zaměstnance. Není limitována počtem pracovníků, kterým může být přiděleno přístupové oprávnění k CÚeR. V žádosti uvede jméno a příjmení, datum narození nebo rodné číslo, adresu pracoviště a kontaktní údaje svého zaměstnance. Na základě této žádosti jsou generovány přístupové údaje zaměstnancům zdravotní pojišťovny.
Zaměstnanci zdravotních pojišťoven přistupují k CÚeR prostřednictvím informačních systémů zdravotní pojišťovny. Jejich prostřednictvím nahlížejí na stažená data o preskripci a dispenzaci léčiv.
Zdravotní pojišťovny informují SÚKL o ukončení pracovního poměru zaměstnanců, kterým bylo přiděleno přístupové oprávnění k CÚeR. Bývalým pracovníkům je přístup k CÚeR zablokován.
Přístupové údaje jsou zaměstnancům ZP zasílány elektronicky prostřednictvím e-mailu v zaheslovaném souboru, heslo k souboru se odesílá na uvedené mobilní číslo nebo písemně prostřednictvím České pošty do vlastních rukou s dodejkou (příloha č.j. UOOU-07399/18-28 ze dne 20. listopadu 2018).

Pravidla a postup pro manuální zpracování žádostí o přístup do Centrálního úložiště elektronických receptů či Registru pro léčivé přípravky s omezením a je určen pro pracovníky oddělení ERP (Elektronický recept) a OSS (Spisová služba) jsou stanoveny směrnicí **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX** (postup pro zpracování žádostí lékařů, farmaceutů a zdravotních pojišťoven o přístup do CÚeR) **a směrnicí XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX** (postupy dle směrnic auditovány – viz Zpráva z auditu ze dne 26. 11. 2018 – příloha č.j. UOOU-07399/1832 ze dne 7. prosince 2018.

Zdravotní pojišťovna získává z CÚeR data o předpisech a výdejích za své pacienty, tento proces přistupuje k osobním údajům pacienta.

Kontrolou bylo zjištěno, že v tomto procesu se zdravotní pojišťovna přihlásí do CÚeR a požádá o seznam všech předpisů a výdejů za dané období. CÚeR předá pojišťovně za dané období data receptů a výdejů za její pojištěnce – uvedený postup byl kontrolujícími kontrolován ve XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX dne 7. února 2019 – viz str. 22 – 24 tohoto protokolu o kontrole.

Ze **<u>Zprávy z auditu ze dne 26. 11. 2018</u>**, kterou SÚKL předložil Úřadu jako přílohu č.j. UOOU07399/18-32 dne 7. prosince 2018 vyplývá, že v rámci kontroly postupů ve smyslu směrnice **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX** bylo zjištěno, že „vydávání přístupů pro zaměstnance zdravotních pojišťoven (ZP) probíhá obdobným postupem jako pro vydání přístupů pro lékaře, tzn., kdy žádost je podána na webovém formuláři pro lékaře a ze strany SÚKL je provedeno ověření žádosti na ZP, zda je oprávněná – komunikace je nastavena prostřednictvím datových schránek(SÚKL x ZP). *V* případě podání žádosti přímo z datové schránky ZP na formuláři (off-line) a podepsání žádosti elektronickým podpisem statutárním zástupcem není jiné ověřování prováděno. Přístup pracovníků ZP je nastaven pouze v rozsahu pojištěnců dané ZP. V současné době si ZP *data z* CÚER stahují automatizovaně v dávkách. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.
Dle vyjádření vedoucí ERP: Jednotlivé ZP jsme poprvé oslovili dopisem dne 6. 9. 2017, aby nám kromě jiného dodaly jméno pracovníka, kterému bude zasláno heslo (dopisy ve spisu *sukls222957/2017). Vzhledem k* tomu, že reakce přišla pouze ze dvou ZP, oslovili jsme ZP druhým dopisem dne 25. 10. 2017 (dopisy ve spisu sukls269798/2017). Na základě informací od ZP (docházelo emailem, emaily mám archivovány) jsme posílali ZP hesla (odeslané dopisy *ve spi*su sukls305124/2017). Pouze u XXXXXXXXXX došlo k osobnímu předání, ve spisu je scan předávacího protokolu, originál mám u sebe založený".
Dále uvedeno doporučení ve vztahu k vedení spisů o vyřizování žádostí.

Ze <u>Zprávy z auditu</u> v uvedené věci dále vyplývá:
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXX.

Organizace využívání eReceptů ve XXXXXXXXXX

Dne 6. února 2019 proběhlo ve XXXXXXXXXXXXXXXXXXXXXX (dále také „XXXXXXXXXX) ústní jednání a místní šetření (ÚZ z ústního jednání a místního šetření konaného dne 6. února 2019, č.j. UOOU-07399/18-54 + příloha „Organizace využívání eReceptů v XXXXXXX) za účelem doplnění informací vztahujících se k předmětu kontroly, zejména kontroly přístupu do CÚeR, kontrola oprávnění osob přistupujících do CÚeR, nakládání s osobními údaji získanými z uvedeného úložiště a jejich zabezpečení, včetně kontroly logování jednotlivých přístupů.

Pracovníci odboru informačního systému podali kontrolujícím informace vztahující se k přístupům do CÚeR a tyto prezentovali kontrolujícím. Zaslána byla k Úřadu taktéž písemná informace „Organizace využívání eReceptů XXXXXXXXXXXXX“ (č.j. UOOU-07399/18-52 ze dne 7. února 2019.

V rámci výše uvedeného bylo zjištěno:

Žádná služba XXXXXXXX a žádný uživatel XXXXXXXXXX nepřistupují do CÚeR; XXXXXXXX má svůj účet u CÚeR zřízen a organizován podle pravidel SÚKL a pod řízením SÚKL; XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

Postup při zřízení účtu XXXXXX v CÚeR

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

Přístup k účtu XXXXXXXX v CÚeR

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

Převzetí dat eReceptů

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

Postup získání eReceptů (modul):

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

Využití interních dat eRecept uživateli – žádná služba XXXXXX a žádný uživatel XXXXXX nepřistupují přímo do CÚeR.

Interní databáze eRecept je připojena k následujícím aplikacím – revize faktur vykázaných zdravotních služeb; náhled na předepsané a vydané eRecepty.

Zdravotní pojišťovny využívají přístupů do CÚeR, a to k osobním údajům ve smyslu čl. 4 odst. 1 Nařízení a ke zvláštním kategoriím osobních údajů subjektů údajů ve smyslu čl. 9 odst. 2 písm. h) a i) Nařízení svých pojištěnců, v souladu s ustanovením § 81 odst. 1 písm. d) zákona č. 378/2007 Sb., zdravotní pojišťovny jsou ve vztahu k osobním údajům a zvláštním kategoriím osobních údajů svých pacientů zpracovávaným v CÚeR v postavení správce osobních údajů ve smyslu čl. čl. 4 odst. 7 Nařízení a SÚKL je prostřednictvím Centrálního úložiště elektronických receptů povinen „zabezpečit bezúplatně přístup do databáze elektronických receptů zdravotním pojišťovnám za účelem provádění kontrolní činnosti podle zákona upravujícího veřejné zdravotní pojištění“.

Kontrolovaná osoba při předávání osobních údajů a zvláštních kategorií osobních údajů zdravotním pojišťovnám postupuje v souladu s čl. 7 odst. 1, písm. f) Nařízení, neboť při předávání zajišťuje náležité zabezpečení osobních údajů prostřednictvím vhodných technických a organizačních opatření.

Kontrolní zjištění č. 7

Policie ČR

Dle sdělení Kontrolované osoby ze dne 7. prosince 2018, č.j. UOOU-07399/18-32 Policie ČR nemá přístup do CÚeR, předpokládá se předání informací v případě oprávněného požadavku při šetření trestné činnosti, zatím nebyl takový požadavek vznesen, přístup není realizován.

Z přílohy č. 1A Smlouvy o dílo (uzavřené se XXXXXXXXXXXXXXXXX ze dne 16. prosince 2016) – Specifikace procesů (čl. 5 Policie ČR) čl. 5.1 Statistické přehledy vyplývá, že „Statistické přehledy budou obsahovat informace o spotřebách léků s *obsahem* pseudoefedrinu, respektive dalších prekurzorů či látek zneužívaných k výrobě drog. Přehledy budou obsahovat informaci o celkové spotřebě s možností vygenerování souhrnných sestav vydaných léků s *obsahem PSE, resp. pr*ekurzorů či látek zneužívaných k výrobě drog za požadované období a výdeje zájmových léčiv za určené období s možností generování sestav na jednotlivé lékárny. Přehledy bude možné třídit a filtrovat podle různých kritérií.

Systém umožní pracovníkovi Policie ČR k těmto přehledům pouze na základě oprávněného požadavku. Veškeré přístupy pracovníků Policie ČR budou v Systému zaznamenány“.

Z čl. 5.2 Přehled IPLP s obsahem konopí za pacienta a období „Systém umožní získat informaci o vydaném množství IPLP s *obsah*em konopí na konkrétního pacienta. Systém umožní vyhledávání buď podle jména, příjmení, data narození, nebo podle čísla pojištěnce. Pracovník Policie ČR bude mít možnost zadat identifikační údaje kontrolované osoby buď prostřednictvím SW instalovaného na pracovišti Policie ČR, nebo prostřednictvím mobilní aplikace na mobilním zařízení. Systém bude dle legislativy sledovat všechny výdeje IPLP na *pacienta v* posledních 30 dnech (uloženo v *RLPO). V* případě výdeje nějakého množství IPLP *s* obsahem konopí na kontrolovanou osobu se zobrazí pracovníkovi Policie ČR jednotlivé uskutečněné výdej s identifikací druhu IPLP s obsahem konopí a s datem výdeje, identifikací předepisujícího lékaře a dále souhrnné množství za posledních 30 dnů“.

Dle č. 5.3 Přehled LP předepisovaných podle zákona o omamných látkách „Systém bude připravený na evidenci statistiku předpisu a výdeje LP předepisovaných podle zákona o omamných látkách. Přehledy musí být dostupné podle různých věkových kategorií, v různém členění a řazení (pacient, množství, datum výdeje, předepisující lékař).

Systém umožní přistoupit pracovníkovi Policie ČR k těmto přehledům pouze na základě oprávněného požadavku. Tento přístup bude vyžadovat povinné zadání zdůvodnění/účelu dotazu např. ve formě zadání čísla jednacího. Veškeré přístupy pracovníků Policie ČR budou *v* Systému zaznamenány“.

Dle čl. 5.4 Přehled LP s omezením „systém bude připravený na evidenci a statistiku předpisu a výdeje LP s omezením. Přehledy musí být dostupné podle různých výběrových kritérií, *v* různém členění a řazení (pacient, množství, datum výdeje, místo výdeje, předepisující lékař). Systém umožní pracovníkovi Policie ČR k těmto přehledům pouze na základě oprávněného požadavku. Tento přístup bude vyžadovat povinné zadání zdůvodnění/účelu dotazu např. *ve* formě zadání čísla jednacího Veškeré přístupy pracovníků Policie ČR budou v Systému zaznamenány“.

Dle čl. 5.5 Přehled LP s obsahem RSE „Systém bude připravený na evidenci a statistiku předpisu a výdeje LP s obsahem PSE, respektive prekurzorů či látek zneužívaných k výrobě drog. Přehledy musí být dostupné podle různých výběrových kritérií, v různém členění a řazení (pacient, množství, datum výdeje, místo výdeje, předepisující lékař).

Systém umožní pracovníkovi Policie ČR k těmto přehledům pouze na základě oprávněného požadavku. Tento přístup bude vyžadovat povinné zadání zdůvodnění/účelu dotazu např. ve formě zadání čísla jednacího Veškeré přístupy pracovníků Policie ČR budou v Systému zaznamenány“.

Dle čl. 5.6 Přehled množství předepsaného LP „Systém bude připravený na zpřístupnění přehledu předpisů konkrétního LP předepsaného konkrétním lékařem (jméno, IČZ). Systém umožní přistoupit pracovníkovi Policie ČR k tomuto přehledu pouze na základě oprávněného požadavku. Tento přístup bude vyžadovat povinné zadání zdůvodnění/účelu dotazu např., ve formě zadání čísla jednacího. Veškeré přístupy pracovníků Policie ČR budou v Systému zaznamenány“.

Dle čl. 5.7 Ověření šarže „Systému bude připravený na ověření šarže léčiva vydaného *v* konkrétním období v konkrétní lékárně.
Systém umožní přistoupit pracovníkovi Policie ČR k tomuto přehledu pouze na základě oprávněného požadavku. Tento přístup bude vyžadovat povinné zadání zdůvodnění/účelu dotazu např., ve formě zadání čísla jednacího. Veškeré přístupy pracovníků Policie ČR budou *v* Systému zaznamenány“.
Dle čl. 5.8 Žádost o opis receptu „Systém umožní na základě oprávněného požadavku přistoupit pracovníkovi Policie ČR k CÚER a po zadání identifikace osoby/pacienta a období či ID eRp získat výpis požadovaných údajů o předepsaných a vydaných LP na danou osobu. Tento přístup bude vyžadovat zadání zdůvodnění/účelu dotazu např. ve formě zadání čísla jednacího. Veškeré přístupy pracovníků Policie ČR budou v Systému zaznamenány".

Ze Zprávy z auditu ze dne 26. 11. 2018, (příloha č.j. UOOU-07399/18-32 dne 7. prosince 2018) vyplývá, že v rámci kontroly postupů ve smyslu směrnice **XXXXXXXXXXXXXXXXXXXXX** bylo zjištěno,
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXX.

Doporučení: 1. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXX,
Poslední komunikace s PČR proběhla v 12/2017, kdy podali žádost o SSL certifikát (nastavení nového přístupu do CÚER“).
Systém umožní pracovníkovi Policie ČR k těmto přehledům pouze na základě oprávněného požadavku. Tento přístup bude vyžadovat povinné zadání zdůvodnění/účelu dotazu např. ve formě zadání čísla jednacího. Veškeré přístupy pracovníků Policie ČR budou v Systému zaznamenány“.
Dle čl. 5. 7 Ověření šarže LP „Systém bude připravený na ověření šarže léčiva vydaného v konkrétním období v konkrétní lékárně. Systém umožní pracovníkovi Policie ČR k těmto přehledům pouze na základě oprávněného požadavku. Tento přístup bude vyžadovat povinné zadání zdůvodnění/účelu dotazu např. ve formě zadání čísla jednacího Veškeré přístupy pracovníků Policie ČR budou v Systému zaznamenány“.

Dle čl. 5.8 Žádost o opis receptu „Systém umožní pouze na základě oprávněného požadavku přistoupit pracovníkovi Policie ČR k CÚER a po zadání identifikace osoby/pacienta a období či ID eRp získat výpis požadovaných údajů o předepsaných a vydaných LP na danou osobu. Tento přístup bude vyžadovat zadání zdůvodnění/účelu dotazu např. ve formě zadání čísla jednacího Veškeré přístupy pracovníků Policie ČR budou v Systému zaznamenány".

Kontrolou bylo ověřeno, že přístupem k RLPO v rámci Policie ČR disponuje Národní protidrogová centrála služby kriminální policie a vyšetřování ve smyslu čl. 3 písm. q) pokynu policejního prezidenta č. 272/2016, tedy formou vzdáleného přístupu disponuje přístupem do RLPO. Z vyjádření Policie ČR ze dne 18. ledna 2019 (Úřad obdržel dne 21. ledna 2019), č.j. PPR-2280-1/ČJ-2019-990300 (č.j. UOOU-07399/18-45) vyplývá: „V praxi to znamená, že pouze operační důstojník Národní protidrogová centrála služby kriminální policie a vyšetřování je oprávněn ke vstupu do tohoto systému, kdy po zadání XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX. K dotazu lze zadat i určité časové období. Odpovědí na dotaz je informace, že konkrétní osoba je nebo není vedena v RLPO. Detailnější informace nejsou Národní protidrogové centrále služby kriminální policie a vyšetřování k *dispozici.*
Přístupem do centrálního úložiště receptů nedisponuje".
Policejní prezidium ČR doplnilo své vyjádření k RLPO dne 5. února 2019, Č.J. uoou-07399/1851 a sdělilo, že: v případě kladné odpovědi na dotaz, zda konkrétní osoba je registrována v předmětné databázi, získá Národní protidrogová centrála služby kriminální policie a vyšetřování ještě informaci o datu vydání a celkovém množství individuálně připravovaného léčivého přípravku s obsahem konopí pro léčebné použití".
Dle ustanovení § 81 odst. 2 zákona č. 37*8/2007 S*b., je centrální úložiště elektronických receptů propojeno s registrem pro léčivé přípravky s omezením podle § 81a za účelem zajištění, dodržování omezení stanoveného v rozhodnutí o registraci podle § 39 odst. 4 písm.
c) a omezení stanoveného prováděcím právním předpisem u individuálně připravovaného léčivého přípravku s obsahem konopí pro léčebné použití.

Kontrolou bylo zjištěno, že Policie ČR nemá přístup do CÚeR, Národní protidrogová centrála služby kriminální policie a vyšetřování ve smyslu čl. 3 písm. q) pokynu policejního prezidenta č. 272/2016, má přístup do RLPO, tedy disponuje přístupem k osobním údajům pacientů ve smyslu čl. 4 odst. 1 Nařízení a zvláštním kategoriím osobních údajů pacientů ve smyslu čl. 9 odst. 1 Nařízení, jimž jsou vydávány léčivé přípravky s omezením nebo individuálně připravovaného léčivého přípravku s obsahem konopí pro léčebné použití, a to na základě oprávněného požadavku (přístup vyžaduje povinné zadání zdůvodnění/účelu dotazu např. ve formě zadání čísla jednacího).

Kontrolující posuzovali oprávnění Policie ČR ke shromažďování osobních údajů a osobních údajů zvláštní kategorie prostřednictvím přístupu k části CÚeR ve které jsou evidovány léčivé přípravky s omezením. Základním právním předpisem je zákon č. 273/2008 Sb., o Policii České republiky, a to zejména jeho ustanovení § 2, § 60 a § 85.

Obecné ustanovení § 2 zákona č. 273/2008 Sb. ukládá Policii ČR sloužit veřejnosti. Jejím úkolem je chránit bezpečnost osob a majetku a veřejný pořádek, předcházet trestné činnosti, plnit úkoly podle trestního řádu a další úkoly na úseku vnitřního pořádku a bezpečnosti svěřené jí zákony, přímo použitelnými předpisy Evropské unie nebo mezinárodními smlouvami, které jsou součástí právního řádu (dále jen „mezinárodní smlouva“).

Dle § 60 odst. 1 zákona č. 273/2008 Sb., zpracovává Policie ČR v souladu s tímto zákonem a jiným právním předpisem informace včetně osobních údajů v rozsahu nezbytném pro plnění svých úkolů.
Dle odst. 2 výše uvedeného ustanovení, musí Policie ČR zpracovávané informace zabezpečit před neoprávněným přístupem, změnou, zničením, ztrátou nebo odcizením, zneužitím nebo jiným neoprávněným zpracováním. Policie dále učiní nezbytná opatření pro zajištění bezpečnosti a spolehlivosti provozovaného informačního systému. Tímto nejsou dotčeny povinnosti podle jiného právního předpisu.

Dle § 85 odst. 1 zákona č. 273/2008 Sb., může Policie ČR při plnění svých úkolů v *souvislosti se* zpracováváním osobních údajů při předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů a zajišťování bezpečnosti České republiky, veřejného pořádku a vnitřní bezpečnosti: ***a)*** zpracovávat nepřesné nebo neověřené osobní údaje; pokud je to možné, policie osobní údaje takto označí, ***b)*** zpracovávat osobní údaje i k jinému účelu, než ke kterému byly shromážděny, ***c)*** shromažďovat osobní údaje otevřeně i utajeným způsobem nebo pod záminkou jiného účelu anebo jiné činnosti, ***d)*** sdružovat osobní údaje, které byly získány k rozdílným účelům, za účelem předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů, zajištění vnitřního pořádku a bezpečnosti včetně pátrání po osobách a věcech a zajištění bezpečnosti České republiky. Dle odst. 2 výše uvedeného ustanovení zpracovává Policie ČR osobní údaje podle odstavce 1 odděleně od osobních údajů zpracovávaných při plnění jiných úkolů policie.

Kontrolou bylo zjištěno, že Policii ČR není umožněn přístup k eReceptům uloženým v CÚeR, tedy přímo do IS eRecept, účelově omezený přístup Policie ČR do Registru léčivých přípravků s omezením, který je ve smyslu § 81a zákona č. 378/2007 Sb. propojen s CÚeR, je Policii ČR umožněn za výše uvedenými účely. Policie ČR je v případě přístupu k osobním údajům a zvláštním kategoriím osobních údajů subjektů údajů zpracovávaným v RLPO v postavení správce osobních údajů a její účelově omezený přístup do RLPO je v souladu s čl. 6 odst. 1 písm. e) Nařízení, neboť „zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce“.
Kontrolovaná osoba při předávání osobních údajů a zvláštních kategorií osobních údajů Policii ČR postupuje v souladu s čl. 7 odst. 1, písm. f) Nařízení, neboť při předávání zajišťuje náležité zabezpečení osobních údajů prostřednictvím vhodných technických a organizačních opatření.

Kontrolní zjištění č. 8

Ministerstvo zdravotnictví ČR

Dle Kontrolované osoby žádný zaměstnanec MZ nemá přístup do CÚeR. MZ získává sumární přehledy o počtu předepsaných a vydaných léčiv pro účely statistické - data jsou sumarizována. Z přílohy č. 1A Smlouvy o dílo (uzavřené se XXXXXXXXXXXXXXXXX ze dne 16. prosince 2016) – Specifikace procesů vyplývá, že „Systém umožní oprávněným pracovníkům přístup k některým statistikám. Jejich počet a obsah bude stanoven“.

Kontrolou bylo zjištěno, že Ministerstvo zdravotnictví využívá pouze sumární přehledy pro účely statistické, tedy nezpracovává osobní údaje pacientů.

Kontrolní zjištění č. 9

Dle čl. 12 odst. 1 Nařízení „Transparentní informace, sdělení a postupy pro výkon práv subjektu údajů správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článcích 13 a 14 a učinil veškerá sdělení podle článků 15 až 22 a 34 o zpracování, zejména pokud se jedná o informace určené konkrétně dítěti. Informace poskytne písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby“.

Dle čl. 14 odst. 1 – Nařízení „Informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů, jestliže osobní údaje nebyly získány od subjektu údajů poskytne správce subjektu údajů tyto informace:

a) totožnost a kontaktní údaje správce a případně jeho zástupce;

b) případně kontaktní údaje případného pověřence pro ochranu osobních údajů;

c) účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování;

d) kategorie dotčených osobních údajů;

e) případné příjemce nebo kategorie příjemců osobních údajů“

Kontrolovaná osoba prostřednictvím http://www.sukl.cz/ochrana-osobnich-udaju zveřejňuje dokument Ochrana osobních údajů (viz příloha č. j. UOOU-07399/18-3 ze dne 12. července 2018) – zveřejněny jsou totožnost a kontaktní údaje správce; jaké osobní údaje jsou zpracovávány; na jakém základě dochází ke zpracování osobních údajů; doba uchování osobních údajů; kdo osobní údaje zpracovává a komu jsou předávány; z jakých zdrojů jsou osobní údaje získávány; jaká jsou práva subjektů údajů, jejichž osobní údaje jsou zpracovávány (právo na přístup; právo na opravu; právo na výmaz; právo na omezení zpracování; právo

vznést námitku proti zpracování; právo podat stížnost); kontakt na pověřence pro ochranu osobních údajů: poverenec@sukl.cz.
Prostřednictvím webových stránek www.sukl.cz je subjektům údajů podána informace prostřednictvím dokumentu „SÚKL je připraven plnit požadavky GDPR“ (http://www.sukl.cz/sukl-je-pripraven-plnit-pozadavkygdpr?highlightWords=pov%C4%9B%C5%99enec+pro+ochranu+osobn%C3%ADch+%C3%BAd aj%C5%AF), a to jakým způsobem se obrátit na SÚKL, v případě, že vznese subjekt údajů dotaz spojený se zpracováním svých osobních údajů. Uvedené opatření je SÚKLem zavedeno za účelem ochrany osobních údajů před jejich předáním neoprávněné osobě.
Poskytování informací upravuje Kontrolovaná osoba ve vnitřní směrnici XXXXXXXXXXXXXXXXX, čl. 6.3.

Kontrolou bylo zjištěno, že Kontrolovaná osoba plní povinnost vyplývající jí jako správci osobních údajů a zvláštních kategorií osobních údajů subjektů údajů z čl. 12 odst. 1 a z čl. 14 odst. 1 Nařízení.

Kontrolní zjištění č. 10

Dle čl. 15 odst. 1 – 4 Nařízení „Subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím:

a) účely zpracování;

b) kategorie dotčených osobních údajů;

c) příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích;

d) plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;

e) existence práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování, anebo vznést námitku proti tomuto zpracování;

f) právo podat stížnost u dozorového úřadu;

g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;

h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů“.

Dle sdělení SÚKL (č.j. UOOU-07399/18-5 ze dne 28. srpna 2018), tento neobdržel žádost subjektu údajů ve smyslu čl. 16 a čl. 21 Nařízení, v běžném režimu dochází pouze k informování SÚKL o změnách příjmení žen – lékařek, lékárnic.

SÚKL neobdržel námitku proti zpracování, v průběhu zpracování nedochází k profilování.

Kontrolou nebylo zjištěno porušení povinností odpovídajících právům subjektů údajů upravených v čl. 15, čl. 16, 17, 18 a 21 Nařízení.

Kontrolní zjištění č. 11

Dle čl. 4 odst. 8 Nařízení je "zpracovatelem" fyzická nebo právnická osoba, orgán veřejné *moci, agentura* nebo jiný subjekt, který zpracovává osobní údaje pro správce“.

Dle čl. 28 odst. 2 Nařízení „Zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce. V případě obecného písemného povolení zpracovatel správce informuje o veškerých zamýšlených změnách týkajících se přijetí dalších zpracovatelů nebo jejich nahrazení, a poskytne tak správci příležitost vyslovit vůči těmto změnám námitky“.

Dle čl. 28 odst. 3 Nařízení **„**Zpracování zpracovatelem se řídí smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Tato smlouva nebo jiný právní akt zejména stanoví, že zpracovatel:

a) zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, p*okud mu* toto zpracování již neukládají právo Unie nebo členského státu, které se na správce vztahuje; v takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;

b) zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;

c) přijme všechna opatření požadovaná podle článku 32

d) dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 a 4;

e) zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených v kapitole III;

f) je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici;

g) v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů;

h) poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje.

Pokud jde o první pododstavec písm. h), informuje zpracovatel neprodleně správce v případě, že podle jeho názoru určitý pokyn porušuje toto nařízení nebo jiné předpisy Unie nebo členského státu týkající se ochrany údajů".

<u>Dle čl. 28 odst. 9 Nařízení</u> **„**Smlouva nebo jiný právní akt podle odstavců 3 a 4 musí být vyhotoveny písemně, v to počítaje i elektronickou formu".

Kontrolovaná osoba za účelem vytvoření Informačního systému e-Recept uzavřela dne 16. 12. 2016 **Smlouvu o dílo** se společností XXXXXXXXXXXXXXXX (viz příloha č.j. UOOU-07399/18-5 ze dne 28. srpna 2018); za účelem poskytování servisní podpory a zajištění rozvoje Informačního systému eRecept uzavřela Kontrolovaná osoba **Smlouvu o poskytování servisní podpory a zajištění rozvoje Informačního systému eRecept** se společností XXXXXXXXXXXXXXXXXXXX ze dne 16. 12. 2016 (viz příloha č.j. UOOU07399/18-5 ze dne 28. srpna 2018).

<u>**Smlouva o dílo** uzavřená mezi **SÚKL** (dále také „Objednatel") **a XXXXXXXXXXXXXXXXXXXXXXX** (dále také „Zhotovitel"),</u> XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX (smlouva vč. Dodatků přílohou č.j. UOOU-07399/18-5 ze dne 28. srpna 2018), uzavřena smlouva o dílo dne 16. 12. 2016 (viz příloha č.j. UOOU-07399/18-5 ze dne 28. srpna 2018 – CD).

Zhotovitel se zavazuje vytvořit IS eRecept (dále také „Systém"). Systém zahrnuje CÚeR dle § 81 zákona o léčivech, registr pro léčivé přípravky s omezením dle § 81 zákona o léčivech a další komponenty.

Čl. 1.2 Dílo tvoří následující části:

Zpracování prováděcího projektu díla; vývoj, dodávka a implementace prototypu aplikačního SW; vývoj a dodávka Systému; implementace Systému v testovacím a referenčním prostředí Objednatele; dodání technické a uživatelské dokumentace; vyškolení uživatelů; zajištění migrace dat; zavedení systému do rutinního provozu

Čl. 9 Ochrana důvěrných informací a osobních údajů:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXX.

<u>Příloha č. 1 Specifikace předmětu díla</u>

V článku 2.2.6 Bezpečnost systému Přílohy č. 1 jsou specifikovány minimální požadavky v oblasti bezpečnosti:

- Systém bude chránit soukromé informace v souladu s příslušnými právními předpisy (zejména Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů a Zákon č. 181/2014 Sb., o kybernetické bezpečnosti), ve znění pozdějších předpisů a bezpečnostní politikou SÚKL
- Každý uživatel bude Systémem jednoznačně identifikován, autentizován a autorizován
- Systém bude umožňovat audit uživatelem provedených operací (včetně pokusů o neautorizované operace)
- Systém bude zajišťovat šifrovanou komunikaci pro webové služby, webové portály (rozhraní) pro uživatele i pro mobilní aplikace
- Zhotovitel dodá bezpečnostní dokumentaci dle kapitoly 3.1.7
- Zhotovitel musí postupovat v souladu s dalšími požadavky v oblasti bezpečnosti dle Přílohy 1B – viz kapitola 7.

V následujících článcích 2.2.6.1 – 7 jsou podrobně specifikovány požadavky v oblastech Důvěrnost, Řízení přístupu, Šifrování, Auditovatelnost, Integrita, Disaster recovery plan (plán obnovení po selhání) a Vývoj.

V článku 3.1.7 Bezpečnostní dokumentace je stanoven minimální obsah bezpečnostní dokumentace takto:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

Bezpečnostní dokumentace byla v rámci kontroly předložena Kontrolovanou osobou jako příloha č.j. UOOU-07399/18-60 ze dne 22. února 2019 -

Z předložené Bezpečnostní dokumentace vyplývá:

Aktualizace 22. 2. 2019

Bezpečnost systému eRecept zohledňuje pro tento případ účelná ustanovení a požadavky normy ISO 27002 a ISO 27034 a vyhlášku č. 316/2014Sb.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

2.1 Způsob řešení autentizace a autorizace externích subjektů:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

2.2 Administrátorský přístup

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxx.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxx.

3.1 Aplikační log

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxx.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxx.

3.2 Log přístupové brány

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxx.

Bod 5. obsahuje Analýzu rizik. V následujících bodech pak jsou detailně popsány:

- 5.3 Bezpečnostní rizika
- 5.5 Identifikace a ohodnocení aktiv
- 5.6 Identifikace hrozeb a zranitelností
- 5.7 Stanovení rizik
- 5.8 Eliminace rizik

Příloha č. 1A k Příloze č. 1 ke Smlouvě o dílo – Specifikace procesů – účelem dokumentu je sumarizace specifikace procesů, které budou řešené v systému e-Recept (dále jen „Systém“) – lékař; lékárník; pacient; zdravotní pojišťovna; Policie ČR; SÚKL; Ministerstvo zdravotnictví..

Z přílohy č. 1A Smlouvy o dílo z čl. 6 SÚKL, 6.1 Specifikace procesů, Statistické přehledy vyplývá, že „Systém umožní pro potřeby SÚKL vytvářet libovolné statistiky prostřednictvím databázových dotazů. Klíčem pro statistiky bude libovolný údaj uváděný na eRp, či zanesený do Systému během výdeje. Jedná se o využití anonymizovaných dat pro účely statistické, analytické či plánovací. V případě legislativního oprávnění i o využití ke kontrolní činnost*i* SÚKL. Například se bude jednat o:

○ Předepsané LP; ○ Vydané LP; ○ Hodnota hrazených a nehrazených LP; ○ Databáze všech uživatelů; ○ *Statistiky z RLPO* ○ Všechny statistiky v libovolném členění (období, lékař, lékárník, pacient, LP, ZP)".

Dodatek č. 1 ke Smlouvě o dílo ze dne 18. 7. 2017 – využití služeb subdodavatele spol. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX (smlouva vč. Dodatků přílohou č.j. UOOU-07399/18-5 ze dne 28. srpna 2018) za účelem řešení nových požadavků na zabezpečení vytvářeného IS v a návaznosti na přijetí Nařízení EP a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Dodatek č. 2 ke Smlouvě o dílo ze dne 13. 11. 2017 – prodloužení lhůt akceptačního řízení.

V rámci kontroly kontrolující obdrželi **Předávací protokoly** ze dne 31. 8. 2017 (zátěžové testy) a 4. 9. 2017 (bezpečnostní testy); dále **Akceptační protokoly** ze dne 3. 8. 2017 (akceptace cílového řešení) a 21. 12. 2017 (akceptace díla) – přílohy č.j. UOOU-07399/18-28 ze dne 20. listopadu 2018 - Předávací protokol, zátěžové testy ze dne 31. 8. 2017, Předávací protokol, bezpečností testy ze dne 4. 9. 2017 a Akceptační protokol, Akceptace cílového řešení, ze dne 3. 8. 2017).

Kontrolou bylo zjištěno, že předmětem akceptace je výstup části díla dle specifikace v odst. 1.2 c) až g) ve Smlouvě o dílo na vytvoření Informačního systému e-Recept uzavřené dne 16. 12. 2016.

Předmět předání odpovídá specifikaci ve Smlouvě a v prováděcím projektu.

Backend CÚeR je nasazen na testovacím i produkčním prostředí, rozhraní je publikováno do internetu a běží v ostrém provozu.

Uživatelské rozhraní pro pacienty, lékaře, Policii ČR, ministerstvo zdravotnictví a správce aplikace je nasazeno na testovacím prostředí SÚKL.

Zajištění přístupu k Základním registrům je otestováno a dočasně pozastaveno do doby nabytí účinnosti novely Zákona
č. 378/2007 Sb, Zákona o léčivech a o změnách některých souvisejících zákonů, která tento přístup přejímajícímu umožní.

Publikace výpisů na CzechPointu a prostřednictvím CzechPoint@home aktuálně neumožňují legislativní překážky. V řešení je tato funkcionalita nahrazena generování výpisu ve webové a mobilní aplikaci pacienta.

Dokumentace k cílovému řešení byla předána přejímajícímu a je vystavena na projektovém WEBu.

Přejímající část díla akceptuje

<u>Akceptační protokol, Akceptace díla, Podklady k akceptaci části díla, ze dne 21. 12. 2017</u>

Kontrolou bylo zjištěno, že v rámci plnění bylo dodáno:

- Systém instalovaný v produkčním prostředí
- Data z původního řešení migrována do produkčního prostředí
- Zátěžové a výkonnostní testy
- Podpora pilotního provozu
- Instalovaný systém v rutinním provozu

Dne 21. 12. 2017 přejímající (XXXXXXXXXXXXXXXXXXXXX) předmět akceptace akceptuje bez výhrad.

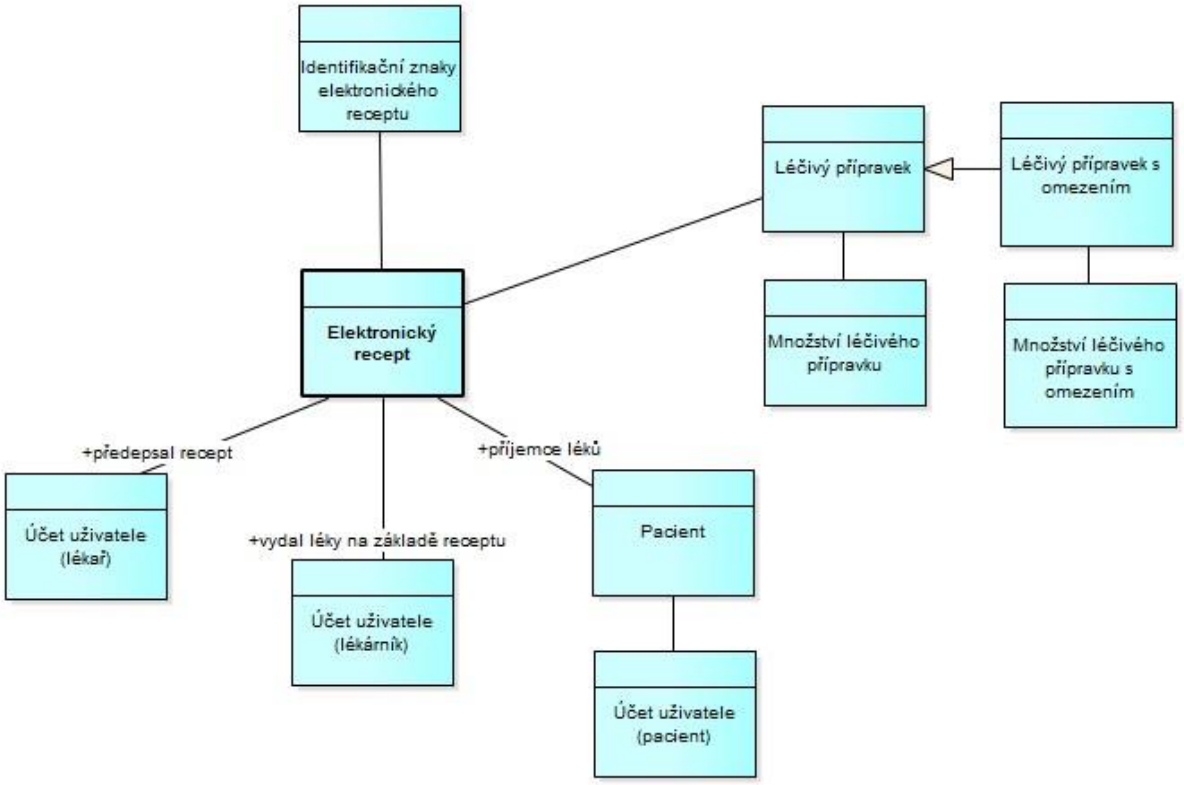
Kontrolovaná osoba v rámci kontroly předložila dokument **<u>Formulář žádosti o stanovisko Hlavního architekta eGovermentu k plánovanému ICT projektu</u>** – typ A, verze 4.2

V části 2.2 Dodržení architektonických principů NA VS ČR obsahuje způsob a míru naplnění 8 principů. Pro princip P3 – Důvěryhodnost je mimo jiné uvedeno:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXX.

V dokumentu jsou dále popsány základní datové modely a to: Datový model externí identity, Datový model léčivého přípravku s omezením a Datový model elektronického receptu, který je uveden následně:



K uloženému elektronickému receptu jsou přiřazeny jeho identifikační znaky, které slouží k jeho dohledání v CÚeR.

V elektronickém receptu jsou uloženy předepsané léčivé přípravky (případně léčivé přípravky s omezením) a jejich předepsané množství.

S e-Receptem je svázán záznam o pacientovi, pro nějž byl e-Recept vystaven. Pokud je pacient registrován jako externí identita, lze záznam o pacientovi provázat s účtem pacienta za účelem poskytnutí e-Receptů pacientovi k prohlížení.

Dále je k elektronickému receptu zapsána informace, jaký lékař vložil e-Recept do CÚER a jaký lékárník e-Recept vyzvedl.

Dále Kontrolovaná osoba předložila **Stanovisko odboru Hlavního architekta eGovermentu k projektu „Informační systém eRecept“** (ze dne 30. května 2016) – souhlasné stanovisko, vydané na základě splnění nutných podmínek pro vydání stanoviska odboru hlavního architekta eGovermentu. Při realizaci projektu požaduje OHA systematické oddělení osobních údajů od údajů eReceptu s logováním přístupu k osobním údajům. Pro každý USE case pak musí být uvedeno, zda přistupuje k osobním údajům pacienta či nikoliv.

Smlouva o poskytování servisní podpory a zajištění rozvoje IS eRecept uzavřená mezi SÚKL (dále také „Objednatel“) **a XXXXXXXXXXXXXXXXXXXX** (dále také „Poskytovatel“), XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, uzavřená dne 16. 12. 2016, (viz příloha č.j. UOOU-07399/18-5 ze dne 28. srpna 2018 – CD).

Čl. 1.01 servisní podpora stanovena na období 48 měsíců od data i nabytí účinnosti této Smlouvy v rozsahu specifikovaném v uvedeném článku.

Čl. 3 Povinnosti Poskytovatele – čl. 3.04 – Poskytovatel se zavazuje předat Objednateli bez zbytečného odkladu po uzavření této Smlouvy seznam osob, které se budou podílet na poskytování Služeb dle této Smlouvy, a to svých pracovníků. Seznam bude vyhotoven pro účely zajištění přístupu do objektu Objednatele. V seznamu budou osoby označeny jménem a příjmením a bude u nich uvedeno označení jejich zaměstnavatele (popř. kontraktora, pokud se nejedná o pracovněprávní vztah). Poskytovatel je povinen předat tento seznam osob *Objednateli s* výslovným souhlasem těchto osob se zpracováním jejich osobních údajů Objednatelem pro účely zajištění přístupu do objektu Objednatele a pro zajištění přístupu *k* příslušným částem informačního systému Objednatele….., Služby dle této Smlouvy v místech Objednatele je Poskytovatel povinen předem domluvit s Objednatelem, o čemž bude pořízen zápis stvrzený podpisy oprávněných osob. Seznam osob je Poskytovatel povinen v případech jakýchkoliv personálních změn neprodleně aktualizovaný předat Objednateli.

Čl. 3.05 V případě, že pro plnění této Smlouvy bude Poskytovatel požadovat pro své zaměstnance, nebo zaměstnance svého subdodavatele přístupová oprávnění k informačním systémům (např. serverům) Objednatele, zavazuje se Poskytovatel neprodleně po vzniku takové potřeby předat Objednateli vyplněnou a podepsanou žádost o přístup do informačního systému. *Poskyt*ovatel je povinen podávat žádosti o přístup/ukončení přístupu do informačního systému Objednatele na formuláři, který je přílohou č. 2 této Smlouvy……. Kopii schválené nebo zamítnuté žádosti předá Objednatel Poskytovateli.

Čl. 3.06 *V souvislosti s* přístupy do informačního systému Objednatele je Poskytovatel dále povinen dodržovat následující povinnosti:

- Poskytovatel je povinen zajistit a odpovídá po celou dobu plnění této Smlouvy Objednateli za to, že do příslušných částí informačního systému Objednate*le budou* fakticky přistupovat pouze osoby, pro něž byla podána žádost o přístup do informačního systému a tato žádost byla schválena manažerem bezpečnosti informací Objednatele ….
- Přidělená oprávnění smí využívat pouze osoba, pro níž byla žádost schválena *ze strany* MBI. Tato osoba nesmí přidělená oprávnění předat žádné jiné osobě…
- Při ukončení pracovního poměru osoby, které měla udělena přístupová práva k Poskytovateli či jeho subdodavateli, je Poskytovatel povinen podat žádost o ukončení přístupu této osoby do informačního systému Objednatele, a to nejpozději do dvou pracovních dnů od okamžiku, kdy rozhodná skutečnost nastane….

Čl. 3.10 Poskytovatel se zavazuje při poskytování Služeb dle této Smlouvy dodržovat veškerá bezpečnostní opatření, týkající se informatických aktiv.

Čl. 8 Subdodávky Poskytovatele – čl. 8.01 Poskytovatel je povinen provádět veškeré plnění podle této Smlouvy výhradně prostřednictvím vlastních zaměstnanců.

Čl. 9 Ochrana důvěrných informací – čl. 9.01 Poskytovatel je povinen zachovávat mlčenlivost o všech skutečnostech, o kterých se dozví při plnění této Smlouvy, a které nejsou právním předpisem určeny ke zveřejnění….

Čl. 9.09 Ve smyslu ustanovení § 4 zákona č. 101/2000 Sb., o ochraně osobních údajů (dále jen „ZOOÚ“), je objednatel správcem osobních údajů obsažených v *S. Pokud Poskytovatel pro* plnění smluvního vztahu nezbytně potřebuje zpracovávat osobní údaje obsažené v Systému, pak se pro účel této Smlouvy stává zpracovatelem osobních údajů.
Čl. 9.11 Poskytovatel není Objednatelem zmocněn ke zpracování osobních údajů obsažených *v* Systému, ledaže by takové zpracování bylo nezbytně potřeba pro účel plnění smluvního *vztahu s* Objednatelem. Poskytovatel je oprávněn zpracovávat osobní údaje pro účel této *Smlouvy pouze v* nezbytném rozsahu a na základě předchozího písemného pověření *Objednatele v souladu s* ZOOÚ.
Čl. 9.12 *Poskytovatel je v* případě, že je Objednatelem pověřen zpracovávat osobní údaje obsažené v Systému, povinen postupovat v souladu se ZOOÚ, zejména:

- Při zpracování osobních údajů dbát, aby subjekty údajů neutrpěly újmu na svých právech….
- Přijmout technická a organizační opatření, aby nemohlo dojít *k* neoprávněnému nebo nahodilému přístupu k osobním údajům… …….
- Zaměstnanci Poskytovatele a další osoby, které by v rámci plnění svých oprávnění a povinností mohli přijít do styku s osobními údaji, jsou povinni zachovávat mlčenlivost o osobních údajích; povinnost mlčenlivosti trvá i po skončení smluvního vztahu.

Čl. 10 Autorská práva

Článek 10.2.1. Udělení licence Poskytovatelem
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

Článek 10.3.1. Udělení licence poskytovatelem
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

Čl. 16 – seznam oprávněných osob smluvních stran pro jednání v záležitostech plnění Smlouvy (novelizováno Dodatkem č. 1 ze dne 19. 7. 2018).

Příloha č. 1 Podrobný popis služeb podpory – katalogové listy.

Dodatek č. 1 ke Smlouvě o poskytování servisní podpory a zajištění rozvoje IS eRecept ze dne 19. 7. 2018 - aktualizace oprávněných osob v čl. 16 odst. 16.01 Smlouvy.

Dodatek č. 2 ke Smlouvě o poskytování servisní podpory a zajištění rozvoje IS eRecept ze dne 23. 8. 2018 – Čl. 2.01 Dosavadní znění odst. 1.01 Smlouvy se doplňuje o následující body: n) Součinnost při ochraně osobních údajů
o) Oznamování incidentu narušení ochrany osobních údajů
p) Oznamování incidentu narušení kybernetické bezpečnosti.
Čl. 2.02 V Čl. 1 Smlouvy se doplňuje nový odstavec 1.04 – Objednatel informuje Poskytovatele, že Systém je prvkem kritické informační infrastruktury ve smyslu § 2 písm. b) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a Objednatel je ve smyslu § 2 písm. e) tohoto zákona správcem tohoto Systému, Poskytovatel toto bere na vědomí a zároveň bere na vědomí, že se po dobu účinnosti této Smlouvy stává provozovatelem Systému ve smyslu § 2 písm. g) zákona o kybernetické bezpečnosti a dle § 3 písm. c) rovněž osobou, jíž jsou v této souvislosti zákona o kybernetické bezpečnosti a příslušnými prováděcími předpisy, zejména vyhláškou č. 82/2018 Sb., ukládány povinnosti v oblasti kybernetické bezpečnosti. Poskytovatel se zavazuje k plnění požadavků stanovených právními předpisy. Poskytovatel se zavazuje k plnění požadavků stanovených právními předpisy dle uvedeného ustanovení při naplňování obsahu bezpečnostní politiky v jeho působnosti.
Dále stanoven rozsah poskytování služeb a režim.

Dosavadní znění Čl. 9 Smlouvy se vypouští a nahrazuje se zněním uvedeným v Dodatku č. 2 - - mlčenlivost; použití důvěrných informací výhradně za účelem splnění svých závazků vyplývajících z této Smlouvy; ochrana důvěrných informací proti jejich neoprávněnému získání třetími osobami, v případě, že Poskytovatel bude mít důvodné podezření, že došlo k neoprávněnému zpřístupnění (získání důvěrných informací; odstranění důvěrných informací v elektronické podobě Poskytovatelem po ukončení Smlouvy; závazek ochrany důvěrných informací v platnosti i po ukončení Smlouvy; Objednatel je správcem osobních údajů obsažených v Systému, pokud Poskytovatel pro plnění smluvního vztahu nezbytně potřebuje zpracovávat osobní údaje obsažené v Systému, pak se pro účel této Smlouvy stává zpracovatelem osobních údajů.

Čl. 9.11 – pokud jde o zpracování osobních údajů nezbytné pro naplnění účelu smluvního vztahu s Objednatelem, je Poskytovatel oprávněn zpracovávat osobní údaje obsažené v Systému pouze na základě písemného pověření Objednatele; písemné pověření musí obsahovat bližší určení typu zpracovávaných osobních údajů, kategorií subjektů údajů, doby trvání zpracování a povahy a účelu zpracování.

Čl. 9.12 Poskytovatel není oprávněn zapojit do zpracování žádný další subjekt bez předchozího výslovného písemného povolení Objednatele.

Čl. 9.13 – povinnosti Poskytovatele při ochraně osobních údajů v době zpracování, je-li Poskytovatel k takovému zpracování písemně pověřen Objednatelem; je-li zapojen další zpracovatel po písemném povolení Objednatelem stanovení je Poskytovatel povinen zajistit, aby tento dodržoval stejné povinnosti k ochraně osobních údajů vyplývající pro Poskytovatele z této Smlouvy; být Objednateli nápomocen pro splnění Objednatelovy povinnosti reagovat na žádosti o výkon práv subjektu údajů vyplývající z platných právních předpisů; poskytování součinnosti Objednateli jím vyžádanou v souvislosti s prováděním technických a organizačních opatření; ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu či subjektu údajů; posuzování vlivu na ochranu osobních údajů; konzultace s dozorovým úřadem ohledně zpracování osobních údajů; ohlásit Objednateli zjištěné porušení zabezpečení zpracovávaných osobních údajů neprodleně, nejpozději do 60 minut od zjištění incidentu…..; umožnit audity, včetně inspekcí, prováděné Objednatelem nebo jiným auditorem, kterého Objednatel pověřil a k těmto auditům přispět svou plnou součinností; informovat neprodleně Objednatele v případě, že dle názoru Poskytovatele určitý pokyn Objednatele porušuje platné právní předpisy týkající se ochrany osobních údajů. Čl. 9.14 Poskytovatel je povinen vést záznamy o činnostech zpracování osobních údajů prováděných pro Objednatele podle příslušných právních předpisů a rovněž vést registr rizik……; Poskytovatel je povinen umožnit Objednateli kdykoliv nahlédnout do vedených záznamů o činnostech zpracování a do obsahu registru rizik a učinit si z nich opis, či výpis.

Čl. 9.15 Poskytovatel prohlašuje, že disponuje veškerým potřebným personálním i technickým zázemím, které poskytuje dostatečné záruky k tomu, že jím prováděné zpracování osobních údajů bude splňovat všechny požadavky platných právních předpisů i této Smlouvy, a je tak schopen zajistit náležitou ochranu práv subjektu údajů.

Čl. 2.08 Dosavadní znění Přílohy č. 1 Smlouvy – Specifikace Služeb se doplňuje o OÚ-1 Součinnost při ochraně osobních údajů. A OÚ-2 Oznamování incidentu narušení ochrany osobních údajů a KB-1 Oznamování incidentu narušení kybernetické bezpečnosti.

Seznam oprávněných osob pro jednání v záležitostech plnění Smlouvy o poskytování servisní podpory a zajištění rozvoje informačního systému e-Recept za SÚKL je uveden v Dodatku č. 1 ke Smlouvě o poskytování servisní podpory a zajištění rozvoje Informačního systému eRecept – viz příloha č.j. UOOU-07399/18-5 ze dne 28. srpna 2018, (dále str. 31 tohoto protokolu o kontrole) – celkem 5 osob, seznam oprávněných osob pro jednání v záležitostech uvedené Smlouvy za Dodavatele Systému (XXXXXXXXXX) je uveden v Dodatku č. 1 ke Smlouvě o poskytování servisní podpory a zajištění rozvoje informačního systému eRecept – celkem 8 osob.

V rámci kontroly byla doložena schválená **žádost o povolení zavedení přidělení přístupu na servery SÚKL** ze dne 12. 3. 2018 (manažerem bezpečnosti informací schválená dne 26. 3. 2018 - (příloha č.j. UOOU-07399/18-32 ze dne 7. prosince 2018) pro 4 zaměstnance XXXXXXXXXXXXXXXXX: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, a to za účelem „Plnění smlouvy o poskytování servisní podpory ze dne 16. 12. 2016 a souvisejících objednávek“, přičemž v Dodatku č. 1 uvedené smlouvy nebyl XXXXXXXX uveden jako osoba oprávněná za smluvní stranu pro jednání v záležitostech plnění smlouvy. Kontrolovaná osoba byla v rámci žádosti o součinnost požádána o vysvětlení uvedeného rozporu. Ze sdělení Kontrolované osoby ze dne 22. února 2019 (č.j. UOOU-07399/18-60) vyplývá, že „uvedení XXXXXXXXXXXXX zaměstnance XXXXXXXXXXXXXXXXXXXXX jako osoby oprávněné přistupovat na servery SÚKL nesouvisí s jeho oprávněním jednat ve věcech smluvních. Osoby, kterým SÚKL udělil oprávnění přístupů k serverům za účelem plnění servisní podpory, jsou odborní pracovníci, zajišťující podporu provozu CÚeR, kteří ovšem nemusí být rozhodnutím svého zaměstnavatele oprávněni jednat za poskytovatele ve věcech smluvních typu uzavírání dodatků, hodnocení plnění smlo*uvy ap*od.“.

Žádost obsahuje závazek, že přístupy lze použít pouze za uvedeným účelem, žadatel a jeho zaměstnanci jsou povinni přístupová oprávnění chránit proti neoprávněnému použití či jakémukoliv zneužití. Současně se zavazují, že informace, se kterými se seznámí, použijí pouze k účelu, pro který jim byl přístup povolen, a nebudou je dále šířit…… Žadatel je povinen SÚKL neprodleně informovat o skutečnosti, že zaměstnanec, kterému bylo přiděleno přístupové oprávnění, přestal pro žadatele vykonávat činnosti, pro něž mu byla přístupová oprávnění udělena……Uchazeč i jeho zaměstnanci přistupující k serverům SÚKL se zavazují k dodržování veškerých povinností stanovených zákonem č. 101/2000 Sb. o ochraně osobních údajů v platném znění, zákona č. 148/1998 Sb. o ochraně utajovaných skutečností v platném znění, a dalších platných právních předpisů. Podpisem této žádosti žadatel osvědčuje, že jeho zaměstnanci jsou plně obeznámeni s povinnostmi stanovenými v právních předpisech dle předchozí věty….

XXXXXXXXX má zřízené administrátorské účty pro schválené administrátory, administrátorské účty neslouží pro přístup k osobním údajům (ustanoveními Smlouvy není oprávněna je používat pro tento účel). Slouží k podpoře při technických problémech, potřebě maintenance. Použití pro účel, kdy by se XXXXXXXXX dostala do role zpracovatele je prováděno předáním konkrétního požadavku do helpdesku, čímž dochází k naplnění ustanovení čl. 9.11 Smlouvy o poskytování servisní podpory.., resp. Dodatku č. 2 - v rámci kontroly byl doložen 3x písemný požadavek v helpdesk- 7. 11. 2018, 16. 11. 2018, 27. 11. 2018 – přílohy č.j. UOOU-07399/18-32 ze dne 7. prosince 2018.
Kontrolou bylo zjištěno, že XXXXXXXXX nezapojila jiného zpracovatele – subdodavatele viz Úřední záznam o provedení kontrolního úkonu ze dne 8. listopadu 2018, č.j. UOOU-07399/18-28.

Kontrolovaná osoba v rámci kontroly předložila dokument **Zpráva z auditu kybernetické bezpečnosti ze dne 16. 10. 2018** (příloha č.j. UOOU-07399/18-22 ze dne 15. listopadu 2018) – čímž Kontrolovaná osoba doložila plnění ustanovení čl. 9.13 Smlouvy o poskytování servisní…., resp. Dodatku č. 2, čl. 9.13.
Z uvedené Zprávy vyplývá:
Cíl auditu: Audit u poskytovatele služeb v roli Provozovatele informačního systému kritické informační infrastruktury – Centrálního úložiště elektronických receptů a významného informačního systému – Registru léčivých přípravků s omezením.
Předmět auditu – prověřit plnění povinností stanovených smlouvu o poskytování servisní podpory a zajištění rozvoje informačního systému eRecept ze dne 16. 12. *2016 a jejich* dodatků a v *souladu s* povinnostmi stanovenými vyhláškou o kybernetické bezpečnosti č. *82/2018 Sb.*
Útvar, místo: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Zjištění:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

2. Hodnocení rizik

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXX.

3. <u>Bezpečnost dat:</u>

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

Doporučení:
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

4. Bezpečnost komunikací
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

5. Řízení vývoje:
Požadavky na realizaci nových funkcionalit jsou zadávány prostřednictvím Helpdesku (HD), kde je vedena i další komunikace a jsou zde uchovávány záznamy (např. analýza požadavku, nacenění, schválení zástupem SÚKL k vývoji). Prezentována byla konkrétní objednávka – Nové menu pro mobilní aplikace……..

6. *Monitoring provozu*
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

7. Plány řízení kontinuity činnosti:
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

8. Způsob likvid*ace dat*
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

9. Ochrana proti škodlivým kódům:
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

Kontrolou bylo zjištěno, že Kontrolovaná osoba za účelem provozu a podpory provozu CÚeR uzavřela smlouvu se společností XXXXXXXXXXXXXXXXXXXX, která je v postavení zpracovatele osobních údajů ve smyslu čl. 4 odst. 8 Nařízení (čl. 9.1 Smlouvy). Uvedená Smlouva je ve smyslu čl. 28 odst. 3 zpracovatelskou smlouvou, přičemž do zpracování osobních údajů v rámci CÚeR nezapojil zpracovatel dalšího zpracovatele. Smlouva obsahuje ujednání ve smyslu čl. 28 odst. 3 písm. b), tj. povinnost mlčenlivosti (čl. 5.7 Smlouvy) Nařízení, čl. 28 odst. 3 písm. c), tj. povinnost přijmout všechna opatření podle čl. 32 Nařízení
(čl. 5.8; čl. 5.9, čl. 5.10, 5.13, čl. 5.18, čl. 9.4, čl. 9.9 Smlouvy, Společnost XXXXXXXXXXXXXXXXXX zpracovává osobní údaje na základě pověření SÚKL dle č. 29 Nařízení a SÚKL jako správce osobních údajů a zvláštních kategorií osobních údajů subjektů údajů provádí kontrolu zpracování, které provádí zpracovatel.

Kontrolou nebylo zjištěno porušení povinností vyplývajících Kontrolované osobě ve smyslu čl. 28 a 29 Nařízení.

Kontrolní zjištění č. 12

Dle čl. 30 odst. 1 Nařízení "Každý správce a jeho případný zástupce vede záznamy o činnostech zpracování, za něž odpovídá". Tyto záznamy obsahují zejména, je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1, dle kterého má správce osobních údajů s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně a) pseudonymizace a šifrování osobních údajů,
b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost systémů a služeb zpracování,
c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů, d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Zabezpečení eReceptu a síťové infrastruktury
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

Kontrolou bylo zjištěno, že Kontrolovaná osoba vede registr rizik – vedeno datum identifikace, stav, opatření, výsledek kontroly opatření, termín další kontroly, vlastník, popis rizika – příloha č.j. UOOU-07399/18-32 ze dne 7. prosince 2018.

<u>Zálohování a archivace dat</u>

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

<u>Logování</u>

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

<u>Kontrolovaná osoba poskytla následující ukázky logování:</u>

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxx.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxx.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxx.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxx.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxx.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxx.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxx.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxx.

Datové centrum

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

Bezpečnostní audity

V rámci kontroly SÚKL předložil:

Zpráva z penetračního testu NIA a identita, provedeného společností XXXXXXXXXXX ze dne 30. srpna 2017.

V rámci tohoto penetračního testu bylo provedeno 14 dílčích testů, pro každý test je popsána metodika, postup, zjištění a případně možné řešení zjištěných zranitelností. Ve shrnutí zprávy

je uvedeno:
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

Auditní zpráva z testu E-Recept lékař, E-Recept Pacient ze srpna 2017.

V rámci tohoto testu bylo provedeno 10 dílčích testů, pro každý test je popsána metodika, postup, zjištění a případně možné řešení zjištěných zranitelností. V souhrnu zprávy jsou uvedena následující rizika:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

Zpráva z penetračního testu ekosystému webových aplikací eRecept, provedeného společností XXXXXXXXXXXXX ze dne 30. srpna 2017.

V rámci testu bylo provedeno 14 dílčích testů. Ve shrnutí zprávy je uvedeno:
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXX.

<u>Zpráva z retestu WSDL 2. kolo testů aplikace eRecept v 1.1, provedeného společností XXXXXXXXXXXX ze dne 2. srpna 2017.</u>

V rámci testu bylo provedeno 15 dílčích testů zaměřených na zranitelnosti zjištěné v předchozím testu. Ve shrnutí zprávy je uvedeno:
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXX.

<u>Penetrační bezpečnostní test realizovaný ve spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost.</u>

Cíle testu:

1. Posouzení vhodnosti a bezpečnosti (na základě poskytnuté technické dokumentace) klíčových částí IT architektury a řešení, které byly při realizaci CÚeR použity.
2. Provedení vnějších testů simulující nepřátelské útoky mající za cíl:

a. Zajistit zabezpečení (dostupnosti/integrity/důvěrnosti) a odolnost CÚeR před vnějšími útoky

b. Ověřit reakce a připravenost monitoringu, jeho obsluh, dotčených osob a subjektů podílejících se na správě a provozu infrastruktury zajišťující komunikaci a funkcionalitu CÚeR.
Testy byly prováděny v období červenec – září 2018 (včetně) a s provedením testů byl seznámen pouze úzký okruh osob, aby ověření reakcí na potencionální útok odpovídalo reálným podmínkám případného útoku.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

Kontrolovaná osoba v rámci kontroly doložila **Program auditů pro rok 2018** – příloha č.j. UOOU-07399/18-32 ze dne 7. prosince 2018 – e-Recept v programu auditů pod č. 13/2018, 9. měsíc 2018, Kontrolovaná osoba zároveň doložila **Zprávu z auditu e-Recept, č. 13/2018** – datum provedení: 19. 9. 2018; 3. 10. 2018; 4. 10. 2018, 23. 10. 2018; 30. 10. 2018; 5. 11. 2018 – zpráva vydána 26. 11. 2018.

V rámci kontroly byla dále předložena tato dokumentace:

XXXXXXXXXXX Žádosti o aktivaci a odblokování účtu, vygenerování nových přístupových hesel či znovu zaslání přístupových údajů do CÚeR (příloha č.j. UOOU-07399/18-60 ze dne 22. února 2019) – vydání 4/09.01. 2019 – stanovení pravidel a postupu pro zpracování žádosti o odblokování účtu, vygenerování nových přístupových hesel či znovu zaslání přístupových údajů do CÚeR. Čl. 6.2 Obecně závazná pravidla pro zpracování žádostí a komunikaci s uživatelem

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

Příkaz ředitele 787/2018 Bezpečnostní politika ze dne 26. 7. 2018 – politika systému řízení bezpečnosti informací; politika řízení aktiv; politika organizační bezpečnosti; politika řízení dodavatelů; politika bezpečnosti lidských zdrojů; politika řízení provozu a komunikací; politika řízení přístupu; politika bezpečného chování uživatelů; politika zálohování a obnovy a dlouhodobého ukládání; politika bezpečného předávání a výměny informací; politika řízení technických zranitelností; politika bezpečného používání mobilních zařízení; politika akvizice, vývoje a údržby; politika ochrany osobních údajů; politika fyzické bezpečnosti; politika bezpečnosti komunikační sítě; politika ochrany před škodlivým kódem; politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí; politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí; politika bezpečného používání kryptografické ochrany; politika řízení změn, politika zvládání kybernetických bezpečnostních incidentů; politik řízení kontinuity činností – zapracování uvedených požadavků jednotlivých politik do vnitřních řídících dokumentů uloženo XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXX Ochrana osobních údajů v SÚKL, vydání 9, ze dne 20. 7. 2018

Čl. 1 Cílem směrnice je zabezpečit ochranu práv fyzických osob při zpracování osobních údajů…. V souladu s požadavky právních předpisů upravujících ochranu osobních údajů zejména pak Obecným Nařízením…..

Směrnice stanovuje povinnosti a kompetence pracovníků SÚKL při procesech zahrnujících zpracování a nakládání s osobními údaji fyzických osob, jež SÚKL jako správce či zpracovatel shromažďuje a zpracovává při výkonu své působnosti.

Majitel procesu je povinen ve spolupráci s Pověřencem průběžně vyhodnocovat dopady této Směrnice a průběžně ji aktualizovat. Ředitel SÚKL se zavazuje jmenovat Pověřence pro ochranu osobních údajů, zajistit mu kompetence a zdroje nezbytné k monitorování činností SÚKL s touto Směrnicí a právními předpisy…..

Čl. 2 Směrnice je závazná pro všechny pracovníky SÚKL, jak jsou definováni v čl. 6.2, písm. i této Směrnice.

Čl. 4 Navazující vnitřní předpisy.

Čl. 5 Související obecně platné předpisy, normy a předpisy EU

Čl. 6 Základní pravidla zpracování osobních údajů – základní zásady; postupy při zpracování osobních údajů; definice a výklad základních pojmů; změny procesů; identifikace a hodnocení rizik při zpracování osobních údajů; zabezpečení osobních údajů; specifické činnosti a opatření; e-mail; záznamy telefonních hovorů; kamerový systém); opatření pro zajištění kontinuity činnosti SÚKL; záznamy o činnostech zpracování; práva dotčených osob (společná pravidla; odvolání souhlasu; námitka; právo na přístup k osobním údajům; právo na opravu; právo na výmaz; právo na omezení zpracování; právo na přenositelnost; právo na přezkum automatizovaného rozhodnutí;); vztahy s dalšími organizacemi (zpřístupnění údajů zpracovateli; zpřístupnění údajů dalšímu správci; zpřístupnění údajů společnému správci;

zpřístupnění jiné osobě s přístupem k údajům; zpracování údajů z pozice zpracovatele); předávání údajů do třetích zemí; bezpečnostní incidenty (vymezení pojmu bezpečnostní incident; odpovědný útvar za řešení bezpečnostního incidentu – Pověřenec; postup řešení incidentu; ohlášení bezpečnostního incidentu dozorovému úřadu; oznámení bezpečnostního incidentu dotčeným osobám; oznámení bezpečnostního incidentu správci; dokumentace bezpečnostních incidentů); součinnost s dozorovým úřadem.

XXXXXXXX Politika v oblasti bezpečnosti informací, vydání 1 ze dne 24. 5. 2018
Čl. 1 Cíl: stanovení bezpečnostní politiky a postupů v oblasti bezpečnosti informací s cílem zabezpečit přísnou ochranu a manipulaci s informacemi, utajovanými skutečnostmi, a ochranu aktiv v SÚKL. Čl. 2 Tento postup je závazný pro všechny pracovníky SÚKL.
Čl. 6 1 – oblast bezpečnosti lidských zdrojů je zajištěna schválenými standardními postupy v oblasti personalistiky, zejména stanovenými ve směrnicích XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.
Čl. 6-1-1 Podmínky zaměstnání – požadavky pro zaměstnání nových pracovníků, včetně požadavků týkajících se bezpečnosti, jsou uvedeny v Pracovním řádu (XXXXXXXXXX) a ve Služebním řádu státních zaměstnanců SÚKL (XXXXXXXXXXXXX).
Čl. 6.1.2. Povědomí o bezpečnosti a školení – v rámci ročního plánu školení jsou stávající pracovníci Ústavu průkazným způsobem školeni v oblasti informační bezpečnosti. Nově nastupující pracovníci, jsou školeni vždy při nástupu do pracovního poměru v Ústavu – seznámení s povinnostmi zaměstnance při nakládání s výpočetní technikou se děje průkazně. Průkaznost je doložena zaměstnancem podepsaným formulářem F-162, který je uložen v osobním spise zaměstnance na PVO. Čl. 6.1.3 Zaměstnanci – každý zaměstnanec bere na vědomí, že prostředky výpočetní techniky svěřené mu Ústavem slouží **výlučně** k účelům plnění pracovních povinností ve prospěch Ústavu.

Dále stanoveno: nastavení hesla; ukládání dat, zákaz připojování jakýchkoliv zařízení ke svěřené technice ani k počítačové síti mimo zařízení schválených; uživatel je povinen při ukončení práce (odchodu ze zaměstnání) vypnout koncovou stanici (PC, Notebook); pravidelná aktualizace přenosného zařízení. Dodržování uvedených požadavků je Ústav oprávněn kontrolovat prostřednictvím MBI (manažer bezpečnosti informací) s využitím monitorovacích nástrojů, transakčních logů a jiných technických a organizačních opatření. Odpovědnost architekta kybernetické bezpečnost.

Čl. 6.2. Politika fyzické bezpečnosti a bezpečnost prostředí – fyzická evidence a její pravidelná aktualizace; umístění serverů v místnosti s řízeným přístupem okruhu nezbytně oprávněných osob, zaměstnanců OIT; vstup zaměstnanců servisních firem pouze v doprovodu zaměstnance OIT.
Čl. 6.2.2. Bezpečnost a ochrana budov XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXX.

Č. 6.2.3. Politika řízení přístupu a práce s mobilními zařízeními a přenosnými nosiči dat – místnosti s výpočetní technikou jsou umístěny v prostorách s řízeným přístupem a jsou zabezpečeny; technická zařízení, elektronická média a listinná dokumentace je uchovávána a v případě potřeby zničena bezpečným způsobem; každý zaměstnanec Ústavu pracuje výhradně pod svým uživatelským účtem, chrání a nesděluje nikomu své přístupové heslo. Čl. 6.2.4. Práce s přenosnými paměťovými médii – použití flash disků pro přenos informací uvnitř Ústavu je povoleno pouze na evidovaných flash discích; na flash disky není povoleno zaznamenávat určené soubory (pokud jsou zaznamenány, musí být zašifrovány); oprávnění používat takový flash má pouze omezený počet prověřených uživatelů, kteří přidělení flash disku budou účelně potřebovat pro plnění pracovních úkolů.

Čl. 6.2.4.5 Uživatelé, kteří nepracují přes VPN, pokud potřebují mimořádně pracovat z domova nebo v terénu, vloží v Ústavu data do notebooku, ten musí být zašifrován; po příchodu do Ústavu importují data do příslušného datového úložiště na serveru.

Čl. 6.2.4.6. Používání „chytrých“ mobilních telefonů, diktafonů apod. podléhá stejným ustanovením jako práce s PC.

Čl. 6.2.5. Přístup k magnetickým mediím pro zálohování dat – přístup omezen, povolený přístup mají pouze vybraní pracovníci.

Čl. 6.2.10. Ochrana zařízení před krádeží – Ústav je chráněn před krádeží zařízená instalovaným EZS, řízeným přístupem do klíčových prostor a nepřetržitou službou ochrany, monitorujícím stav střežených prostor…..

Čl. 6.2.12 Politika v oblasti dodavatelských vztahů – zapracování a ošetření bezpečnosti informací a s tím spojené požadavky na třetí strany posuzuje v rámci postupů daných XXXX i MBI.

Čl. 6.2.13. Řízení servisních služeb a údržby – veškeré externí služby jsou najímány smluvně a požadavky na bezpečnost jsou ve smlouvách uvedeny….

Čl. 6.3.4. Politika zálohování – zálohování je popsáno v dokumentu XXXXXXXXXXXXXXX Postupy v oblasti IT a IS.

Čl. 6.3.5. Bezpečnost při zacházení s médii

Čl. 6.3.5.1. Likvidace médií – fyzická likvidace provozně neupotřebitelných; o likvidaci je veden záznam (v rámci kontroly předložena 2x příloha z 15. 11. 2018 – Protokol číslo 443/2018 o likvidaci datových souborů na přenosném médiu – harddisk -fyzická likvidace ze dne 25. 7. 2018; Protokol číslo 509/2018 o likvidaci datových souborů na přenosném médiu – USB Flashdisk XXXXXXXXXXXXXXXXXXXX ze dne 2. 11. 2018 – příloha č.j. UOOU-07399/18-22 ze dne 15. listopadu 2018).

Čl. 6.3.5.2. Politika ochrany informací – Postupy pro manipulaci s informacemi – pro zabránění neautorizovanému přístupu nebo zneužití informací jsou stanoveny postupy pro manipulaci s nimi a pro jejich ukládání – viz XXXXXXXXXX Spisový a skartační řád, XXXXXXXXX Aprobační řád.

Čl. 6.3.5.3. Systémová dokumentace je bezpečně uložena a chráněna před zneužitím v elektronické formě na serveru. Za aktualizaci a úplnost dokumentace odpovídá OIT.

Čl. 6.4. Politika řízení přístupu

Čl. 6.4.1. Přístup k informacím a procesům Ústavu je řízen bezpečnostními a provozními požadavky (XXXXXXXXXXXXXXXXXXXXXXXXX).

XXXXXXXXXXXXXX Manuální zpracování žádostí o přístup do CÚ ER RLPO ZP PČR

Dokument stanovuje pravidla a postup pro manuální zpracování žádostí o přístup do Centrálního úložiště elektronických receptů či Registru pro léčivé přípravky s omezením a je určen pro pracovníky oddělení ERP (Elektronický recept) a OSS (Spisová služba). V dokumentu jsou odděleně definovány jednotlivé kroky zřizování přístupových oprávnění pro pracovníky zdravotních pojišťoven (ZP) a Policie České republiky (PČR - přístup k RLPO), počínaje způsobem podání žádosti a konče aktivací přístupu.

Pro zpracování žádostí o přístup pracovníků ZP je pro každou Činnost předepsáno kdo Provádí/Zodpovídá a co je Vstupem a Výstupem dané činnosti.

Pro zpracování žádostí o přístup pracovníků PČR je pro každý Krok předepsán Popis činnosti, kdo Provádí a Nástroje.

Postup dle směrnice auditován – viz Zpráva z auditu zed ne 26. 11. 2018 – příloha č.j. UOOU07399/18-32 ze dne 7. prosince 2018.

XXXXXXXXXXX vydani Aprobacni rad(1)

Cílem tohoto dokumentu je upravit zásady a pravidla pro podepisování písemností (v listinné i elektronické podobě) vyhotovených, schvalovaných a odesílaných v rámci Ústavu i mimo něj; upravit zásady a pravidla pro používání razítek, zejména evidence úředních razítek (se státním znakem), jiných razítek než úředních – služebních, určení osob odpovědných za jejich držení a použití, definice dokumentů, na které jsou tato razítka použita, a opatření k zamezení zneužití razítek; upravit zásady a pravidla pro používání průkazu inspektora, zejména evidence a určení osob odpovědných za jejich držení a použití a opatření k zamezení zneužití; stanovit zásady pro použití malého státního znaku na písemnostech; definovat klasifikaci dokumentů podle důvěrnosti, politiku a postupy pro nakládání s dokumenty dle klasifikace.

Dokument je určen všem zaměstnancům SÚKL.

XXXXXXXXXX vydani Spisovy a skartacni rad(8)

Účelem spisového a skartačního řádu je zabezpečit řádný, rychlý a účelný chod spisové služby v Státním ústavu pro kontrolu léčiv (dále jen SÚKL nebo Ústav), umožňující jednoznačnou identifikaci písemností a spisů, jejich pohotové vyhledávání v kterémkoliv stádiu jejich vyřizování, uložení až po jejich vyřazení ve skartačním řízení. Ochranu osobních údajů při vedení spisové služby v podmínkách SÚKL upravuje směrnice XXXXXXXXXX Ochrana osobních údajů v SÚKL.

Tímto řádem se řídí všichni zaměstnanci SÚKL a osoby vykonávající práce pro SÚKL. Za plnění úkolů daných tímto řádem každému jednotlivému útvaru odpovídá jeho vedoucí.

XXXXXXXXXXXX vydani Uzavirani smluv

Cílem je stanovit pravidla pro jednotný postup procesu přípravy, projednání a schvalování smluv a jejich dodatků (dále jen „smlouva“) uzavíraných Státním ústavem pro kontrolu léčiv (dále jen „SÚKL“), včetně postupu při získávání stanovisek odborných útvarů k návrhům smluv a jejich dokumentaci. Cílem je taktéž posílit právní jistotu SÚKL v postavení smluvní strany při uzavírání smluv vznikajících při jeho činnosti a zvýšit právní vědomí zaměstnanců SÚKL. Článek 6.4.2 Postup interního posouzení uvádí: Manažer pro bezpečnost informací zkontroluje, zda znění smlouvy zaručuje ochranu SÚKL z hlediska bezpečnosti informací a zda znění smlouvy vyhovuje právním přepisům upravujícím bezpečnost informací, a to zejména, nikoli však výlučně, s ohledem na plnění povinností uložených zákonem o kybernetické bezpečnosti.

XXXXXXXXXX vydani System managementu bezpecnosti informaci

Účelem směrnice je stanovení rozsahu a popis Systému managementu bezpečnosti informací (ISMS – Information Security Management System), který je součástí integrovaného systému managementu organizace Státní ústav pro kontrolu léčiv (dále jen „Ústav“). Současně směrnice slaďuje a stanovuje principy realizace ISMS tak, aby v Ústavu byla dodržována zákonná ustanovení a požadavky legislativy ošetřující provozování informačních systémů (zejména Zákon č. 181/2014 o kybernetické bezpečnosti a Vyhláška č. 316/2014 o kybernetické bezpečnosti).
Směrnice je závazná pro všechny pracovníky Ústavu.

XXXXXXXX vydání Ochrana osobních údajů v SÚKL

Cílem směrnice je zabezpečit ochranu práv fyzických osob při zpracování osobních údajů, předcházet neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich nežádoucí změně, zničení či ztrátě, neoprávněnému přenosu nebo neoprávněnému zpracování a zajištění ochrany soukromí fyzických osob v souladu s požadavky právních předpisů upravujících ochranu osobních údajů zejména pak **Obecným Nařízením 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)** (dále jen „GDPR“) a příslušných vnitrostátních právních předpisů upravujících ochranu osobních údajů.

Tato Směrnice stanovuje povinnosti a kompetence pracovníků Státního ústavu pro kontrolu léčiv („Ústav“) při procesech zahrnujících zpracování a nakládání s osobními údaji fyzických osob, jež Ústav jako správce či zpracovatel shromažďuje a zpracovává při výkonu své působnosti.

Majitel procesu je povinen ve spolupráci s Pověřencem průběžně vyhodnocovat dopady této Směrnice a průběžně ji aktualizovat. Ředitel Ústavu se zavazuje jmenovat Pověřence pro ochranu osobních údajů, zajistit mu kompetence a zdroje nezbytné k monitorování souladu

činností Ústavu s touto Směrnicí a právními předpisy chránícími osobní údaje, umožnit v souvislosti se zpracováním osobních údajů Pověřenci přístup k vedení Ústavu, zapojit ho do všech relevantních procesů, zohlednit jeho názor a doporučení v otázkách ochrany osobních údajů a v případě odchylného postupu tento postup zdůvodnit.

Článek 6.0 definuje Základní zásady zpracování osobních údajů, v článku 6.1 jsou definovány Postupy při zpracování osobních údajů. V článku 6.5 Zabezpečení osobních údajů je uvedeno:

a. Pokud pracovník přijde do styku s osobními údaji, je povinen o nich zachovávat mlčenlivost. Pracovníci jsou povinni zachovávat mlčenlivost jak o samotných osobních údajích, tak také o bezpečnostních opatřeních přijatých na jejich ochranu. Povinnost mlčenlivosti trvá i po skončení pracovněprávního či služebního vztahu pracovníka, nebo po ukončení příslušných smluvních činností pro Ústav. Porušení povinnosti mlčenlivosti bude posuzováno podle příslušných právních předpisů.

b. Pracovníci útvarů, v nichž probíhá zpracování osobních údajů a ostatní pracovníci, jež při se plnění svých pracovních úkolů mohou dostat do styku s osobnímu údaji, musejí absolvovat školení o ochraně informací a osobních údajů, a podepsat příslušný dokument o ochraně osobních údajů. Pracovníkem podepsaný dokument je uložen v osobním spise zaměstnance vedeném PVO.

c. Pracovníci mají přístup k osobním údajům pouze v případě, že je to nutné pro plnění jejich pracovních či smluvních povinností. Omezení práva přístupu pracovníků k osobním údajům druhých osob musí dodržováno.

d. Pro zabezpečení osobních údajů, jsou platná všechna ustanovení politiky bezpečnosti informací obsažené v XXXXXX beze zbytku

e. Případné stížnosti subjektů údajů na porušení povinností Ústavu při ochraně osobních údajů prošetří Pověřenec nebo ředitel Ústavu, případně podle potřeby v součinnosti další určený vedoucí pracovník. Zjistí-li prošetřující osoba oprávněnost stížnosti, učiní neprodleně opatření k nápravě. Následně informuje ředitele, kdo porušení povinností Ústavu při ochraně osobních údajů způsobil a jaká konkrétní opatření k nápravě byla učiněna. O opatřeních k nápravě informuje též stěžovatele případně další dotčenou osobu

V článku 6.7 Specifické činnosti a opatření jsou pak stanovena pravidla pro e-mail, záznamy telefonních hovorů a kamerový systém.

XXXXXXXXXX vydani Sluzebni rad statnich zamestnancu SUKL(3)

Služební řád zakládá povinnosti státních zaměstnanců Ústavu výlučně v rámci obecně závazných předpisů nebo předpisů vydaných služebním orgánem v nadřízeném služebním úřadu nebo náměstkem pro státní službu. Služební řád je závazný pro všechny státní zaměstnance Ústavu, kteří jsou k němu ve služebním poměru, jakož i pro zaměstnance v pracovním poměru vykonávající činnosti podle § 5 služebního zákona (Služba a obory služby). Služební řád neobsahuje specifická ustanovení, týkající se nakládání s osobními údaji.

XXXXXXXXXXXXX vydání Zpracování žádostí do systému CÚ ER

Cílem předpisu je stanovit pravidla a postup pro zpracování žádostí lékařů, lékárníků a zdravotních pojišťoven o přístup do Centrálního úložiště elektronických receptů. V článku 6.4

Proces zpracování žádosti jsou stanoveny jednotlivé Činnosti od přijetí žádosti o zřízení přístupu po notifikaci o aktivaci účtu, resp. zamítnutí žádosti. Pro každou Činnost je stanoveno, kdo Provádí/Zodpovídá a co je Vstupem a Výstupem dané Činnosti.
Postup dle směrnice auditován – viz Zpráva z auditu ze dne 26. 11. 2018 – příloha č.j. UOOU07399/18-32 ze dne 7. prosince 2018.

XXXXXXXXXXX vydani_Postupy_v_oblasti_IT_a_IS_navrh_DS
Dokument stanovuje postupy v oblasti informačních technologií (IT) a informačních systémů (IS) v organizaci Státní ústav pro kontrolu léčiv (dále jen SÚKL) a je určen pro pracovníky OIT (Odbor informačních technologií). čl. 6.3.1 Správa výměnných médií
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

čl. 6.3.2 Likvidace médií
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

čl. 6.3.3 Přeprava fyzických médií
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXX.

čl. 6.4.12.7.1 Zaznamenávání událostí formou logů
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXX.

čl. 6.4.12.7.2 Ochrana logů
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXX.

čl. 6.4.12.7.3 Logy o činnosti administrátorů a operátorů
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXX.

XXXXXXXXXXXXXXXXX je dosud nevydaný interní Standardní postup, kdy důvodem nevydání je očekávání zpřesňujícího rozsahu požadavků národní právní úpravy ČR implementující požadavky Obecného nařízení (EU) 2016/679. Požadavky uvedeného Nařízení, u nichž Kontrolovaná osoba neočekává další přesnění, jsou přeneseny do vnitřních procesů a podmínek ve směrnici XXXXXXXX.

Kontrolou nebylo zjištěno porušení povinností ve smyslu ustanovení čl. 30 odst. 1 Nařízení, neboť doložila plnění povinností ve smyslu uvedeného článku.

Kontrolní zjištění č. 13

Dle čl. 32 odst. 1 Nařízení správce nebo zpracovatel „Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, **nebo neoprávněný přístup k *nim***“.

Bezpečnostní incident

Dne 9. 3. 2018 došlo k bezpečnostnímu incidentu NEDOSTUPNOSTI CÚeR po dobu cca 7590 minut. Incident byl v souladu s požadavky Vyhlášky č. 316/2014 Sb., nahlášen Národnímu úřadu pro kybernetickou a informační bezpečnost včetně popisu příčiny a přijatých opatření.

Dle sdělení SÚKL byla v souvislosti s uvedeným incidentem provedena tato opatření:

- bylo provedeno další školení pracovníků call centra a zvýšení jejich odbornosti v dané problematice, zvláštní důraz byl soustředěn na komunikaci v krizových situacích
- pro rychlejší orientaci v problému a zajištění rychlé a korektní informovanosti veřejnosti byly vytvořeny typizované odpovědi pro možné případy omezení dostupnosti jakékoli komponenty CÚeR pro call centrum i tiskové oddělení
- byla provedena revize všech interních předpisů a došlo k jejich aktualizaci
- byla provedena revize interní komunikační matice, její aktualizace a nastavení kompetencí, eskalačních úrovní a správných toků informací
- byl vytvořen nový interní předpis pro krizovou komunikaci (krizový manuál) v případě částečné či úplné nedostupnosti CÚeR nebo některých jeho komponent
- byla provedena revize komunikační matice s dodavateli, její aktualizace
- proběhlo zlepšení aktivního monitoringu všech komponent CÚeR i souvisejících infrastrukturních prvků a systémů
- bylo provedeno doplnění webových stránek www.epreskripce.cz o informaci o aktuálním stavu provozu CÚeR (semafor)
- průběžně jsou na webových stránkách www.epreskripce.cz zveřejňována doporučení pro výrobce SW třetích stran, která mají minimalizovat případné problémy při výpadky některého ze systémů
- byl vytvořen aktuální seznam krizových emailových adres výrobců SW třetích stran, profesních komor a významných zdravotnických zařízení, na který je v případě problému s nedostupností CÚeR zaslána notifikační zpráva (postup je popsán v krizovém manuálu)

Kontrolní zjištění 13 A

Bezpečnostní incidenty – zneužití přístupových oprávnění

V rámci ústního jednání a místního šetření v SÚKL dne 8. listopadu 2018 uvedli zástupci Kontrolované osoby, že k Úřadu pro ochranu osobních údajů bylo zasláno **oznámení o bezpečnostním incidentu, který byl zjištěn dne 24. 10. 2018** (příloha č.j. UOOU-07399/1822 ze dne 15. listopadu 2018 – popis incidentu) – velký počet přístupů v lékárně, podán návrh na zablokování účtu.

Kontrolovaná osoba k Úřadu zaslala kopie hlášení pro Úřad (ve smyslu čl. 33 Nařízení EU), příloha č.j. UOOU-07399/18-22 ze dne 15. listopadu 2018 – předána kopie hlášení o incidentu ze dne 25. října 2018 (č.j. 365055/18-sukl); dále Kontrolovaná osoba poskytla písemnou informaci o incidentu (postup XXXXXXXXXX); podezření od dodavatele eRecept - Dne 23. října 2018 zadala XXXXXXXXXXXXXXXXXXXXXXXX - na základě ověření obdržel SÚKL od společnosti XXXXXXXXXX doporučení k ověření bezpečnostní hrozby na velký počet přístupů (327 556 tis.), a to od dubna 2018 do 25. října 2018 – analýzou příčin bylo zjištěno, že aktivita je

generována využíváním internetové aplikace XXXXXXXX; Kontrolovaná osoba zároveň doložila 3 doplňující zprávy – komunikace pracovníků SÚKL ve věci bezpečnostního incidentu – Narušení důvěrnosti/únik informací; 2x printscreen náhledu. Doplněno informací ze dne 7. prosince 2018, č.j. UOOU-07399/18-32 ze dne 7. prosince 2018.

Z ohlášení incidentu při zabezpečení zpracování (os. údajů) ve smyslu čl. 33 Nařízení (EU) 2016/679 zaslaného k Úřadu dne 25. října 2018 (příloha č.j. UOOU-07399/18-22 ze dne 15. listopadu 2018, popis incidentu) vyplývá, že dne 24. 10. 2018 „bylo při kontrole bezpečnostních požadavků stanovených při provozování Centrálního úložiště elektronických receptů (CÚER) zjištěno **porušení důvěrnosti** osobních údajů, kategorie zvláštní (citlivé) údaje. *K* uvedenému incidentu došlo porušením uživatele – lékárnice, které byly vydány přístupové údaje tím, že tato poskytla své přihlašovací údaje SW *aplikaci XXXXXXXXXXXX k* širokému použití uživatelům aplikace***. V* důsledku toho, se mohl kdokoliv znalý kódu receptu dostat k *jeho* elektronickému záznamu.** Aplikace mu následně zobrazila následující údaje:

- křestní jméno
- první písmeno příjmení (ostatní příjmení nahrazena hvězdičkou)
- všechny na receptu předepsané léky Jde o XXXXXXXXXXX.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXX.

Přijaté opatření – Účet uvedené lékárnice byl zablokován, bude vyzvána ke změně hesla a opětovně poučena o povinnosti zachovávat přístupové údaje tak, aby nebyly zneužitelné (neumožnila jejich využití) jinou osobou.
Incident byl hlášen rovněž Národnímu úřadu pro kybernetickou a informační bezpečnost“.

Kontrolou bylo zjištěno, že hlášení o bezpečnostním incidentu bylo zasláno k NÚKIB dne 25. října 2018 (účet byl zablokován 26. října 2018).

Dne 8. listopadu 2018 byl zjištěn bezpečnostní incident – kdy stejný provozovatel lékáren společnost XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX získává od zaměstnankyň – lékárnic jimi provozovaných lékáren přístupové údaje umožňující náhled do Centrálního úložiště elektronických receptů jakékoliv osobě znající nebo náhodně uhodnuvší kód receptu. S ohledem na opakovaný způsob zneužití přístupu k citlivým údajům subjektů údajů, na potenciální rozsah a skutečnost, že přístup mají v plném rozsahu i správci (nelékárnici) aplikace XXXXXXXXXXXX, vyhodnotil SÚKL incident jako velmi závažný – kritický.

Kontrolovaná osoba k Úřadu zaslala kopie hlášení pro Úřad (ve smyslu čl. 33 Nařízení EU), příloha č.j. UOOU-07399/18-22 ze dne 15. listopadu 2018 – předána kopie hlášení o incidentu k Úřadu ze dne 9. listopadu 2018; dále Kontrolovaná osoba poskytla záznam o projednání incidentu s XXXXXXXXXXXXX; dopis provozovateli lékáren, který těžil z incidentů zneužití přístupů k CÚeR; doplněnou písemnou informaci o incidentu (XXXXXXXXXXXXXX) - č.j. UOOU-07399/18-32 ze dne 7. prosince 2018 – z uvedené informace Kontrolované osoby dále vyplývá, že byl proveden náhodný pokus na straně SÚKL, zda aplikace XXXXXXXX neumožňuje po zablokování účtu XXXXXXXXXXXX funkcionalitu, která není v souladu s požadavky zákona o léčivech na účel zřízení a provozování CÚeR. Dne 8. 11. 2018 v 19,50 bylo identifikováno, že XXXXXXXX opět umožňuje používání aplikace; 9. 11. 2018 9,03 identifikován účet uživatele, pod kterým je přistupováno, jako XXXXXXXXXXXXX; účet byl zablokován. Dne 9. 11. 2018 9,29 zadán požadavek na SD jako bezpečnostní incident; 9. 11. 2018 11,07 vyjádření pana Kusovského, souhlas se zablokováním přístupů; informace o osobním projednání s paní magistrou, incident nahlášen na Úřad.
Dále Kontrolovaná osoba k incidentu uvedla, že XXXXXXXXXX využívá přístup na dvou pracovištích (pracuje ve dvou lékárnách), ke zneužití došlo na pracovišti (lékárně) řetězce XXXXXXXXXXX. Počet přístupů pod tímto účtem činil v kontrolovaném období 1. – 8. 11. 2018 **87 přístupů.**

Z ohlášení incidentu při zabezpečení zpracování (os. údajů) ve smyslu čl. 33 Nařízení (EU) 2016/679 zaslaného k Úřadu dne 9. listopadu 2018 (č.j. 379409/18-sukl), (příloha č.j. UOOUUOOU-07399/18-22 ze dne 15. listopadu 2018) vyplývá, že dne 8. 11. 2018 „bylo při kontrole bezpečnostních požadavků stanovených při provozování Centrálního úložiště elektronických receptů (CÚER) zjištěno porušení důvěrnosti osobních údajů, kategorie zvláštní (citlivé) údaje. Jde o opakování incidentu hlášeného dne 25. 10. 2018 pod. č.j. sukl355302/2018, kdy stejný provozovatel lékáren XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX (dále „společnost XXXXXXXXXXX“) získává od zaměstnankyň – lékárnic jimi provozovaných lékáren přístupové údaje **umožňující náhled do Centrálního úložiště elektronických receptů jakékoliv osobě znající nebo náhodně uhodnuvší kód receptu.**
Veřejnosti je pak umožněno nahlédnout na následující údaje receptu:

- křestní jméno pacienta
- první písmeno příjmení pacienta (ostatní příjmení nahrazena hvězdičkou)
- všechny na receptu předepsané léky
- křestní jméno lékaře, který recept vystavil
- první písmeno příjmení lékaře, který recept vystavil (ostatní příjmení nahrazena hvězdičkou)

Správci aplikace XXXXXXXXXX, kteří přihlašovací údaje do aplikace implementovali, ***mohou*** **nahlížet na plné osobní (a citlivé) údaje pacienta a lékaře,** ač nejde ani o odborné *praco*vníky – lékárníky. V tomto identifikovaném incidentu poskytla v *rozporu s pokyny, za* kterých byly přístupové údaje vydány (nepřenositelnost) XXXXXXXXXXXXXXXX.

S ohledem na opakovaný způsob zneužití přístupu k citlivým údajům subjektu údajů, na potencionální rozsah a skutečnost, že přístup mají v plném rozsahu i správci (nelékárníci) aplikace XXXXXXXXXXX hodnotíme **INCIDENT JAKO VELMI ZÁVAŽNÝ – Kritický a dáváme Úřadu pro ochranu osobních údajů podnět k zahájení řízení pro porušení ochrany osobních údajů *ve s*polečnosti XXXXXXXXXXXX i lékárnicemi, které poskytly své přihlašovací údaje k účelům, které nejsou stanoveny Zákonem o léčivech v platném znění.**

Přijaté opatření – Účet uvedené lékárnice byl zablokován, bude vyzvána ke změně hesla a opětovně poučena o povinnosti zachovávat přístupové údaje tak, aby nebyly zneužitelné (neumožnila jejich využití) jinou osobou. Společnost XXXXXXXXXXX bude upozorněna na nezákonnost svého počínání.

Incident byl hlášen rovněž Národnímu úřadu pro kybernetickou a informační bezpečnost".

Kontrolovaná osoba předložila Záznam o projednání incidentu ze dne 13. 11. 2018 – XXXXXXXXXXXXXXXX vysvětlena podstata způsobeného incidentu spočívající zejména v tom, že předáním svých přihlašovacích údajů osobám, které nejsou uvedeny ve výčtu oprávněných osob dle § 82 Zákona o léčivech, umožnila jejich přístupy do centrálního úložiště elektronických receptů v rozporu s účely, které stanovuje tento zákon. XXXXXXXXXXX byly na základě její žádosti předány nové přihlašovací údaje s poučením o jejich nepřenositelnosti a nemožnosti poskytovat je jakékoliv jiné osobě.

Kontrolovaná osoba zaslala dopis provozovateli lékáren – XXXXXXXXXXXXXX ze dne 12-listopadu 2018 (č.j. 382780/18-sukl) – kromě jiného uvedeno z právního výčtu § 82 zákona č. 378/2007 Sb., že „nevyplývá účel, pro který byl poskytnutý přístup využíván Vaší společností na internetových stránkách XXXXXXXXX, kdy umožnil přístup správcům těchto stránek *k* osobním údajům v kategorii zvláštní (citlivé) osobní údaje a další využití i pro jiné účely než stanoví uvedený Zákon.

Tím, že přístupové údaje byly využity pracovníky spravující internetové stránky, kteří nejsou ani lékaři, ani lékárníci – došlo k závažnému bezpečnostnímu incidentu ohrožení bezpečnosti zvláštní kategorie osobních údajů ve smyslu Obecného Nařízení Evropského parlamentu a *Rady* (EU) č. 2016/679o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů), (dále jen Nařízení GDPR), a to požadavku čl. 32 odst. 1 písm. b).

Účty obou magister, které poskytly své přístupové údaje do centrálního úložiště osobních údajů, byly zablokovány a Úřadu pro ochranu osobních údajů jsme předali podnět k zahájení řízení pro porušení uvedeného Nařízení GDPR. Další rozhodování o podnětu k zahájení řízení o porušení ochrany zvláštní kategorie osobních údajů je v kompetenci Úřadu pro ochranu osobních údajů.

Státní ústav pro kontrolu léčiv jako správce Centrálního úložiště elektronických receptů Vás tímto důrazně upozorňuje na právní úpravu podmínek účelu, pro který je úložiště zřízeno a právní požadavky upravující ochranu osobních údajů, nimž jsou vázáni Vaši zaměstnanci a zaměstnankyně ve všech pracovních pozicích".

<u>Ze sdělení SÚKL ze dne 8. ledna 2019</u> (č.j. UOOU-07399/18-39) vyplývá, že incident ze dne 25. 10. 2018 byl **detekován** v rámci monitoringu počtu přístupů uživatelů systému CÚeR (lékařů/lékárníků, kdy počet přístupů jedné z uživatelek (XXXXXXXXXX) byl v řádech vyšší než u jiných uživatelů. Nástroj XXXXXXXX – jeho pravidla pro detekci incidentů byla následně rozšířena pro monitoring takovýchto případů.
Druhý incident (XXXXXXXXXXX) byl již detekován pracovníky OIT SÚKL právě v důsledku rozšíření pravidel XXXXXXXXX a navíc průběžnou kontrolou mobilní aplikace XXXXXXXXX, zda neumožňuje neoprávněné přístupy k údajům CÚeR.
Z uvedeného sdělení SÚKL vyplývá, že 100% prevence tohoto typu incidentu na úrovni technicko-organizačních opatření není možná. Jde vždy o selhání jednotlivce, který oprávnění přístupu získá řádně, avšak v rozporu s poučením dopustí zneužití individuálních přístupových údajů jinou osobou.
Přílohou č.j. UOOU-07399/18-39 ze dne 8. ledna 2018 zaslal SÚKL printescreen obrazovky mobilní aplikace XXXXXXXXXX, kde je zobrazeno, jaké údaje mohl vidět uživatel aplikace, který získal neoprávněně přístup., ten byl pořízen dle sdělení SÚKL nativní vlastností mobilního telefonu, na kterém byl rozsah incidentu posuzován. Dále bylo sděleno, že okruhy osob v uvedeném incidentu jsou fakticky dva:

1. osoby užívající aplikaci XXXXXXXXXX (převážně pacienti – držitelé kódu receptu), kdy tyto osoby měly přístup k údajům v rozsahu přiloženého printscreenu.
2. Je nutno dle sdělení SÚKL brát v potaz i skutečnost, že tvůrci aplikace XXXXXXX (IT specialisté) mohli mít přístup k údajům naprosto identický, jaký má lékárnice – zneviditelnění části jména a příjmení bylo výsledkem až jimi vytvořené aplikace.

V rámci ústního jednání dne 23. listopadu 2018 (Úřední záznam o provedení kontrolního úkonu, č.j. UOOU-07399/18-35) byly od SÚKL vyžádány informace týkající se „registrace“ klientských systémů pro lékaře a lékárníky a zda před registrací byla SÚKLem provedena kontrola či testování těchto systémů z hlediska zranitelnosti IS eRecept a doložení analýzou rizik, současně byla vyžádána informace, jaký systém využívá společnost XXXXXXXXXXXXX. K uvedenému SÚKL sdělil, že pojem „Registrace“ klientského systému, jak je míněn na webu ePreskripce informuje jeho potencionální uživatele, že je kompatibilní s centrálním systémem. Tedy, že jeho užití klientem je funkční pro rozsah jeho přístupu k CÚeR. XXX.

Přílohou sdělení SÚKL ze dne 8. ledna 2019 (č.j. UOOU-07399/18-39), zaslal SÚKL kopii dopisu adresovaný Ing. Z. Kusovskému, MBA dne 23. 11. 2018 – vyjádření XXXXXXX, člena představenstva XXXXXXXXXXX ve věci i týkající se „údajného" ohrožení ochrany osobních údajů, ke kterému mělo dojít tím, že XXXXXXXXXXX (zaměstnankyně společnosti) poskytla této společnosti své identifikační přístupové údaje do Centrálního úložiště elektronických receptů. V dopise je kromě jiného uvedeno: „XXXXXXXXXXXXX své identifikační přístupové údaje do Centrálního úložiště elektronických receptů (dále jen „CUER") skutečně za účelem zajištění fungování Služby (služba erecept.XXXXXXXXXXX) poskytla, nikoli však způsobem, jak vyplývá z Vašeho sdělení, nýbrž tak, aby byl naplněn účel CUER uvedený v *ust.* § 81 odst. 1 písm. c) a d) zákona o léčivech a zároveň nedošlo k jejich zneužití. Přístupové údaje byly poskytnuty na bázi zaměstnanec – zaměstnavatel, a to přímo jejich zadáním do softwaru Služby. Údaje nejsou nikde zaznamenány a nenachází se na žádném datovém ani hmotném nosiči. Ze softwaru Služby je navíc nelze zpětně získat a je tak zcela vyloučena možnost, aby kdokoliv přístupové údaje XXXXXXXXXXXXX zneužil. Přístup do CUER je navíc možný jen v případě, kdy daná osoba má jednak přístup k identifikačním údajům lékárníka (v našem případě), ale zároveň i k SSL certifikátu, který byl přidělen naší společnosti za účelem zajištění přístupu do CUER. Je tedy vyloučena i možnost zneužití samotné služby, protože přístupové údaje a současně i SSL certifikát má k dispozici výlučně lékárník (pro jistotu zde znovu opakujeme, že identifikační údaje nejsou nikde zaznamenány, má je k *dispozici jen* XXXXXXXXX).
Poskytnuté údaje tedy loužily výlučně k zajištění Služby pro zákazníka, shodně jako například u programu XXXXXXXXXX, který funguje na obdobném principu, a výlučně pro potřeby farmaceuta provádějícího vydej léčiva ve smyslu výše citovaného ustanovení zákona o léčivech. Jejich zneužití bylo zcela znemožněno, a to jednak díky samotnému nastavení přístupu do CUER, který požaduje několikanásobné ověření přístupu, ale rovněž díky procesům nastaveným *v* rámci naší společnosti k identifikačním údajům XXXXXXXX byl teoreticky možný, stále by *se jednalo o situaci v* rámci společnosti a nehrozil by únik takové informace mimo ni. Každý zaměstnanec naší společnosti má v pracovní smlouvě uloženu povinnost mlčenlivosti a porušení takové povinnosti by bylo vnímáno jako důvod pro ukončení pracovního poměru".

SÚKL v reakci na výše uvedené vyjádření společnosti XXXXXXXXXXXX přípisem č.j. Sukls372538-2/2018 ze dne 21. prosince 2018 kromě jiného sdělil, že ze společností uváděných ustanovení zákona o léčivech § 81odst. 1, písm. c) a d) jednoznačně plyne, že přístupové údaje měly sloužit výlučně farmaceutovi (paní XXXXXXXXXXX) pro účel výdeje léčivého přípravku. Žádný jiný účel, umožňující předání individuálně vydaných přístupových údajů svému zaměstnavateli ani jiné osobě pro jiný účel než vydání léčivého přípravku, ustanovení § 81 zákona o léčivech nepřipouští. Tím méně lze považovat za souladný se zákonem postup, kdy jsou přístupové údaje, přidělené individuálně určenému farmaceutovi za účelem jeho přístupu do centrálního úložiště elektronických receptů, zadány do komerčního softwarového nástroje odlišného od centrálního úložiště elektronických receptů. Dále ve sdělení SÚKL uvedeno: „Zablokování přístupových oprávnění paní XXXXXXXXXX bylo nutným bezpečnostním opatřením správce k naplnění požadavků na zabezpečení zvláštní kategorie osobních údajů ve smyslu ustanovení čl. 32 odst. 1 písm. B) Obecného Nařízení a Rady (EU) č. 2016/679o ochraně fyzických osob v

souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů). Údaje o léčivých přípravcích předepsaných konkrétní identifikované osobě je nepochybně nutno považovat za zvláštní kategorii osobních údajů ve smyslu čl. 9 obecného nařízení o ochraně osobních údajů, neboť se jedná o údaje vypovídající o jeho zdravotním stavu. Zablokováním přístupových oprávnění paní XXXXXXXXX došlo též k naplnění povinnosti ústavu, uložené v § 81 písm. E) zákona o léčivech: „zajistit ochranu a bezpečnost v databázi uložených elektronických receptů před jejich poškozením, zneužitím nebo ztrátou podle zvláštního právního předpisů. Realizované bezpečnostní opatření současně naplnilo požadavky stanovené v ust. § 12, odst. 2, písm. B) a § 17 písm. A) vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti".

Úřad ve věci obou bezpečnostních incidentů a na základě informace Kontrolované osoby, že ve věci ohlásila uvedené bezpečnostní incidenty **Národnímu úřadu pro kybernetickou a informační bezpečnost (dle také „NÚKIB"),** požádal o součinnost NÚKIB přípisem č.j. UOOU-07399/18-30 ze dne 20. listopadu 2018. Úřad uvedeným přípisem požádal NÚKIB o vyjádření k uvedeným bezpečnostním incidentům. NÚKIB v odpovědi na žádost o poskytnutí součinnosti Úřadu dne 10. prosince 2018 (č.j. UOOU-07399/18-34) sdělil: „Kybernetické bezpečnostní incidenty, k nimž se váže Vaše žádost, byly Národnímu úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB") hlášeny Státním ústavem pro kontrolu léčiv (dále jen „SÚKL") jako správcem informačního systému kritické infrastruktury ve smyslu § 3 písm. c) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „zákon o kybernetické bezpečnosti"). SÚKL tak dostál povinnosti mu uložené ustanovením § 8 odst. 1 zákona o kybernetické bezpečnosti. *Vzhledem k* tomu, že bylo ze strany SÚKL zneužití přístupových údajů zjištěno, klasifikováno jako kybernetický bezpečnostní incident a nahlášeno NÚKIB, lze se domnívat, že zafungoval bezpečnostní mechanismus. SÚKL komunikoval se zaměstnanci NÚKIB, od kterých ***dostal*** **doporučení ke zvýšení bezpečnostního opatření k přístupu do centrálního úložiště elektronických receptů například pomocí zavedení dvoufaktorové autentizace, která může zamezit opakování tohoto incidentu**".

Dne 13. února 2019 SÚKL v rámci webových stránek zveřejnil informaci „Jak správně zacházet se svými přidělenými přístupovými údaji k informačnímu systému eRecept?", uvedeny jsou informace o způsobu, jak je nutné zacházet s přístupovými údaji do IS eRecept, které jsou SÚKL zasílány koncovým uživatelům: „Přístupové údaje koncového uživatele se skládají z přihlašovacího jména a hesla, které uživatel obdrží od SÚKL, přičemž **heslo je nutné si při prvním přihlášení změnit.**

Přístupové údaje je nutné udržovat v důvěrnosti tak, aby se zamezilo jejich zneužití***. V*** **žádném případě přístupové údaje nikomu nesdělujte.** Pokud jako uživatel systému eRecept sdělíte třetí osobě své přístupové údaje, poskytujete této osobě možnost komunikovat se systémem eRecept Vaším jménem ***a v*** **rozporu se zákonem umožníte této osobě přístup do systému eRecept.** Takovým krokem ztrácíte nad přístupovými údaji kontrolu a dochází ke kompromitaci Vašeho účtu se všemi negativními důsledky, které z *toho* plynou. Kompromitace účtu může

mít za následek též bezpečnostní opatření ze strany SÚKL *v* podobě zablokování příslušných přístupových údajů.
Ztrátu či vyzrazení Vašich přístupových údajů je třeba bezodkladně hlásit SÚKL a současně požádat o obnovu přístupových údajů (viz Otázky a odpovědi, dotaz č. „1“), čímž budou původní přístupové údaje zneplatněny a obratem Vám budou vydány nové.
Přístupové údaje nesmí být koncovým uživatelem využívány k jiným účelům, než ke kterým mu byly vydány, tl. Pouze k takovým účelům, které vyplývají z příslušných právních předpisů. Zneužití přístupových údajů k nezákonnému účelu je postižitelné podle příslušných právních předpisů. Důrazně doporučujeme, abyste ke svým přístupovým údajům k informačnímu systému eRecept přistupovali se stejnou opatrností, s jakou se chováte například *k* přístupovým údajům do internetového bankovnictví, k *PIN* kódu Vaší platební karty, či *k* jiným důležitým přístupovým údajům, **jejichž zneužití by pro Vás mohlo mít vážné negativní následky.** Jedná se o přístupové údaje vydané pro Vás jako konkrétní fyzickou osobu, které slouží k přístupu k informačnímu systému, který je prvkem kritické informační infrastruktury státu, a je tudíž nutné s nimi zacházet se vší vážností a obezřetností“.

Kontrolou bylo zjištěno, že zaměstnankyně společnosti XXXXXXXXXXXXXX, XXXXXXXXXX XXXXXXXXXXXXXXX tím, že předaly informace o přístupových údajích, které obdržely jako lékárnice ve smyslu § 81 zákona č. 378/2007 Sb., společnosti XXXXXXXXXXXXXX, která je zapracovala do mobilní aplikace „XXXXXXXXXX“, svým jednáním ohrozily bezpečnost osobních údajů a zvláštních kategorií osobních údajů subjektů údajů zpracovávaných v CÚeR, čímž porušily povinnost dle čl. 29 Nařízení.

Kontrolující shodně s Národním úřadem pro kybernetickou a informační bezpečnost konstatují, že SÚKL na základě přijatých opatření detekoval narušení zabezpečení osobních údajů a dle čl. 33 Nařízení oba incidenty Úřadu nahlásil, včetně informace o postupu při vyřizování incidentu.
Současně kontrolující konstatují, že k narušení bezpečnosti došlo na základě nedostatečných přijatých bezpečnostních opatření při přístupu do CÚeR, tj. Kontrolovaná osoba nepřijala opatření, která by zamezila použití neoprávněně předaných přístupových oprávnění., tím došlo k porušení povinnosti dle čl. 32 odst. 1 Nařízení, neboť s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, neprovedl dostatečná vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, a to zejména zavedením dvoufaktorové autentizace.

Kontrolní zjištění 13 B

Kontroly prováděné SÚKL v lékárnách

V rámci kontroly bylo zjištěno, že SÚKL provádí prostřednictvím inspektorů SÚKL kontroly lékáren jejichž předmětem je především dodržování správné lékárenské praxe (dále viz níže Protokol o kontrole), kontrola využívání přístupových oprávnění do CÚeR se děje v případech, kdy vznikají pochybnosti, zda vydávající osoba je k tomu oprávněná podle příslušného ustanovení zákona č. 378/2007 Sb., o léčivech, v platném znění.
Kontrolující si od Kontrolované osoby vyžádali kopii protokolu o kontrole provedené inspektory SÚKL, Kontrolovaná osoba předložila:

Protokol o kontrole ze dne 28. 11. 2018 (příloha č.j. UOPOU-007399/18-60 ze dne 22. února 2019), přičemž kontrolovanou osobou byla XXXXXXXXXXXXXX, kontrola byla provedena v XXXXXXXXX XXXXXX.
Předmětem kontroly bylo plnění požadavků zákona č. 378/2007 Sb., o léčivech a změnách některých souvisejících zákonů (zákon o léčivech), ve znění pozdějších předpisů (dále jen „zákon o léčivech“) a jeho prováděcích předpisů; zákona č. 167/1998 Sb., o návykových látkách a o změně některých dalších zákonů, ve znění pozdějších předpisů; zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů a vyhlášky č. 92/2012 Sb., o požadavcích na minimální technické a věcné vybavení zdravotnických zařízení a kontaktních pracovišť domácí péče; zákona č. 40/1995 Sb., o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb., o provozování rozhlasového a televizního vysílání, ve znění pozdějších předpisů a zákona č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, ve znění pozdějších předpisů, na základě podnětu ke kontrole, který byl Ústavu doručen dne 08. 11. 2018 v souvislosti s podezřením na zacházení s léčivými přípravky neoprávněnou osobou.
Kromě jiného z protokolu čl. 3.7 vyplývá, že „Kontrolou záznamů v elektronické evidenci lékárny bylo dále zjištěno, že v období od 15. 10. 2018 do data kontroly dne 09. 11. 2018 byly realizovány výdeje léčivých přípravků na elektronické recepty jménem XXXXXXXXX, který se *v* lékárně již nevyskytoval a dle sdělení XXXXX zemřel dne 15. 10. 2018. Provozovatel lékárny *v* uvedeném období dle sdělení XXXXXXXXX nedisponoval v systému PC jiným kvalifikovaným certifikátem oprávněné osoby farmaceuta pro přístup do centrálního úložiště elektronických receptů, kromě osoby zesnulého XXXXXXXXX a XXXXXXXXXX, která již pro provozovatele lékárny činnosti farmaceuta nevykonává, jak je doloženo PrintScr*een obrazovky PC se* seznamem certifikátů (příloha č. 5). Tím, že došlo ke zneužití přístupových práv XXXXXX, vydaných výlučně jemu a pro účel použití daný ustanovením§ 81 odst. 1 písm. c) zákona č. 378/2007 Sb. jinou osobou, a byl tak této osobě umožněn přístup k osobním údajům kategorie zvláštní (citlivé) osobní údaje, došlo k porušení ochrany osobních údajů při jejich zpracování ve smyslu Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, o ochraně fyzických osob v *souvislosti* se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů) („Nařízení GDPR“). O této skutečnosti je Státní ústav pro kontrolu léčiv jako správce centrálního úložiště elektronických receptů povinen informovat Úřad pro ochranu osobních údajů“.

Kontrolovaná osoba v rámci své kontrolní činnosti konstatovala, že došlo ke zneužití přístupových práv neoprávněnou osobou, která nebyla lékárníkem. Kontrolující konstatují, že Kontrolovaná osoba nemá dle platné právní úpravy žádnou možnost takovému jednání zabránit. Současně je nezbytné konstatovat, že povinnost příslušné komory (ČLK, ČSK, ČLeK) potvrdit SUKL platnost členství žádajícího lékárníka o přidělení přístupových oprávnění do CÚeR vyplývá z pouze z podzákonných předpisů SUKL, přičemž žádný předpis neobsahuje povinnost uloženou profesním komorám (ČLK, ČSK, ČLeK) sdělovat SUKL informaci o ukončení členství svého člena, resp. zákon č. 220/1991 Sb. o České lékařské komoře, České stomatologické komoře a České lékárnické komoře, přičemž příslušné profesní komory (ČLK, ČSK, ČLeK) nemají přístup do centrálních evidencí (ROB), tedy neexistuje možnost ověřovat, zda člen komory nezemřel a tedy přestal být dle § 8 zákona č. 220/1991 Sb. členem komory. Rovněž neexistuje žádná oznamovací povinnost třetích osob vůči komorám. Tedy v daném případě provozovateli lékárny, pozůstalým apod., že došlo k úmrtí člena komory.

V daném případě kontrolující konstatují, že byly neoprávněně využity pro přístup do CÚeR přístupové údaje zemřelého lékárníka XXXXXXXX, který je obdržel jako lékárník ve smyslu § 81 zákona č. 378/2007 Sb., a to provozovatelem lékárny, čímž mohlo dojít k porušení povinnosti dle čl. 29 Nařízení.

Kontrolovaná osoba v rámci své kontrolní činnost detekovala neoprávněný přístup do CÚeR, přičemž nemá možnost zjistit, že osoba, které byly přiděleny přístupové údaje do CÚeR tyto již z výše uvedených důvodů nemůže užívat, tedy v uvedeném případě nebylo zjištěno porušení povinností Kontrolované osoby, a to ani dle čl. 30, resp. 32 Nařízení.

Kontrolní zjištění č. 14

Dle čl. 37 odst. 1 písm. a) Nařízení Správce a zpracovatel jmenují pověřence pro ochranu osobních údaj, kdy zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimk*ou* soudů jednajících v rámci svých soudních pravomocí.

Kontrolou bylo zjištěno, že Kontrolovaná osoba jmenovala pověřence pro ochranu osobních – Pověření ze dne 12. 7. 2017 – příloha č.j. UOOU-07399/18-12ze dne 6. listopadu 2018.
Úkoly, pravomoci a postavení pověřence pro ochranu osobních údajů jsou stanoveny směrnicí XXXXXXX Ochrana osobních údajů v SÚKL, čl. 6.2 (příloha č.j. UOOU-07399/18-5 ze dne 28. srpna 2018).

Kontrolou nebylo zjištěno porušení čl. 37 odst. 1 Nařízení, neboť Kontrolovaná osoba pověřence jmenovala a oznámila Úřadu.

Kontrolní zjištění č. 15

Dle čl. 37 odst. 7 Nařízení Správce nebo zpracovatel zveřejní kontaktní údaje pověřence pro ochranu osobních údajů a sdělí je dozorovému úřadu.

Kontrolou bylo zjištěno, že dne 26. 5. 2018 bylo emailem č.j. UOOU-06600/18-108 Úřadu oznámeno, že pověřencem pro ochranu osobních údajů je Ing. Zdeněk Kusovský, MBA.
Kontaktní údaje zdenek@kusovsky@sukl.cz, tel. 272 185 241.
Úřad obdržel dne 21. 6. 2018 prostřednictvím datové schránky oznámení č.j. UOOU06600/18-629 o ustanovení Ing. Zdeňka Kusovského, MBA do funkce Pověřence pro ochranu osobních údajů SÚKL na základě Pověření ze dne 12. 7. 2017.
Dále bylo kontrolou zjištěno, že na stránce http://www.sukl.cz/ochrana-osobnnich-udaju je uvedena e-mailová adresa poverenec@sukl.cz a na stránce http://www.sukl.cz/sukl/reditel-r je uvedena e-mailová adresa poverenec(at)sukl.cz.

Kontrolou nebylo zjištěno porušení ustanovení čl. 37 odst. 7 Nařízení, neboť Kontrolovaná osoba prostřednictvím dálkového přístupu zveřejnila kontaktní údaje pověřence pro ochranu osobních údajů.

Podklady, ze kterých kontrolní zjištění vycházejí

Spisová dokumentace č.j. UOOU-07399/18

Poučení o opravném prostředku

Proti kontrolnímu zjištění uvedenému v protokolu o kontrole může kontrolovaná osoba podat kontrolnímu orgánu ve lhůtě 15 dnů ode dne doručení protokolu o kontrole námitky. Námitky se podávají písemně, musí z nich být zřejmé, proti jakému kontrolnímu zjištění směřují, a musí obsahovat odůvodnění nesouhlasu s tímto kontrolním zjištěním.

Pokud kontrolující inspektorka nevyhoví námitkám ve lhůtě 7 dnů ode dne jejich doručení, vyřídí je předsedkyně Úřadu ve lhůtě 30 dnů ode dne jejich doručení.

Protokol o kontrole je vypracován ve dvou vyhotoveních. Jedno vyhotovení bude doručeno Státnímu úřadu pro kontrolu léčiv formou stejnopisu, druhé vyhotovení bude založeno jako originál s podpisem kontrolujících v kontrolním spisu č.j. UOOU-07399/18. V tomto spisu jsou rovněž založeny všechny podklady uvedené ve sběrném archu kontrolního spisu pod pořadovým číslem 1 – 62.

V rámci této kontroly bylo kontrolujícími kontrolováno a prověřováno výhradně zpracování osobních údajů v čase provedení kontroly, uvedeném v tomto protokolu o kontrole.

Podpisová doložka

Otisk

úředního

razítka

Kontrolující:

PaedDr. Jana Rybínová	inspektorka Úřadu	(dokument podepsán elektronicky)
……		……
jméno a příjmení		podpis
JUDr. Michal Jelínek	pověřený zaměstnanec Úřadu	(dokument podepsán elektronicky)
……..		……..
jméno		podpis
	pověřený	
Ing. Max Gůt	zaměstnanec Úřadu	(dokument podepsán elektronicky)
……		……..
jméno		podpis

Předpis

Lékař	Lékárník	Pacient	Zdravotní pojišťovna	Atribut
Ano	Ano	Ano	Ano	Příznak receptu Akutní
Ano	Ano	Ano	Ano	datum vystavení
Ano	Ano	Ano	Ano	doporučující lékař - jméno/jména
Ano	Ano	Ano	Ano	doporučující lékař - příjmení
Ano	Ano	Ano	Ano	doporučující lékař - identifikační číslo pracoviště PZS
Ano	Ano	Ano	Ano	doporučující lékař - identifikační číslo zařízení PZS
Ano	Ano	Ano	Ano	doporučující lékař - DIČ poskytovatele zdravotních služeb
Ano	Ano	Ano	Ano	doporučující lékař - IČ poskytovatele zdravotních služeb
Ano	Ano	Ano	Ano	doporučující lékař - název poskytovatele zdravotních služeb
Ano	Ano	Ano	Ano	doporučující lékař - telefon poskytovatele zdravotních služeb
Ano	Ano	Ano	Ano	doporučující lékař - ID odbornosti
Ano	Ano	Ano	Ano	ID elektronického předpisu GUID – vzniklý ve starém dočasném řešení (odpovídá poli EIDE z DR VZP přímo, nebo po případné konverzi z čárového kódu)
Ano	Ano	Ano	Ano	ID elektronického předpisu zkrácený - vzniklý v novém finálním řešení (odpovídá poli EIDE z DR VZP)

Ano	Ano	Ano	Ano	počet celkových výdejů/počet opakování
Ano	Ano	Ano	Ano	hmotnost pacienta
Ano	Ano	Ano	Ano	číslo pojištěnce
Ano	Ano	Ano	Ano	email pacienta

Ano	Ano	Ano	Ano	způsob notifikace pacienta
Ano	Ano	Ano	Ano	název věznice pacienta
Ano	Ano	Ano	Ano	pohlaví pacienta
Ano	Ano	Ano	Ano	telefon pacienta
Nepoužívá se	Nepoužívá se	Nepoužívá se	Nepoužívá se	příznak digitalizovaného předpisu (digitalizované předpisy nemají uvedené položky)/ Momentálně se nepoužívá
Ano	Ano	Ano	Ano	platnost předpisu do
Ano	Ano	Ano	Ano	poznámka k předpisu
Ano	Ano	Ano	Ano	předepisující lékař - email lékaře
Ano	Ano	Ano	Ano	předepisující lékař - identifikační číslo pracoviště v rámci PZS
Ano	Ano	Ano	Ano	předepisující lékař - identifikační číslo zařízení PZS
Ano	Ano	Ano	Ano	předepisující lékař - název oddělení poskytovatele zdravotních služeb
Ano	Ano	Ano	Ano	předepisující lékař - jméno/jména
Ano	Ano	Ano	Ano	předepisující lékař - příjmení
Ano	Ano	Ano	Ano	PZS: předepisující lékař - část obce

Ano	Ano	Ano	Ano	PZS: předepisující lékař - číslo evidenční
Ano	Ano	Ano	Ano	PZS: předepisující lékař - číslo orientační
Ano	Ano	Ano	Ano	PZS: předepisující lékař - číslo popisné
Ano	Ano	Ano	Ano	PZS: předepisující lékař - obec
Ano	Ano	Ano	Ano	PZS: předepisující lékař - okres
Ano	Ano	Ano	Ano	PZS: předepisující lékař - PSČ
Ano	Ano	Ano	Ano	PZS: předepisující lékař - ulice
Ano	Ano	Ano	Ano	PZS: předepisující lékař – DIČ poskytovatele zdravotních služeb
Ano	Ano	Ano	Ano	adresa pacienta - obec
Ano	Ano	Ano	Ano	adresa pacienta - okres
Ano	Ano	Ano	Ano	adresa pacienta - PSČ
Ano	Ano	Ano	Ano	adresa pacienta - ulice
Ano	Ano	Ano	Ano	datum narození pacienta
Ano	Ano	Ano	Ano	jméno/jména pacienta
Ano	Ano	Ano	Ano	příjmení pacienta
Ano	Ano	Ano	Ano	Druh pojištění pacienta
Ano	Ano	Ano	Ano	Druh dokladu pacienta
Ano	Ano	Ano	Ano	Číslo dokladu pacienta

Léčivé přípravky na předpise

Lékař	Lékárník	Pacient	Zdravotní pojišťovna	Atribut
Ano	Ano	Ano	Ano	název HVLP/neregHVLP/IPLP/INN
Ano	Ano	Ano	Ano	cesta podání HVLP/neregHVLP/IPLP/INN
Ano	Ano	Ano	Ano	forma HVLP/neregHVLP/INN
Ano	Ano	Ano	Ano	množství HVLP/neregHVLP/INN
Ano	Ano	Ano	Ano	síla HVLP/neregHVLP/INN
Ano	Ano	Ano	Ano	počet balení HVLP/neregHVLP/INN
Ano	Ano	Ano	Ano	návod (XXXX)
Ano	Ano	Ano	Ano	příznak Nezaměňovat
Ano	Ano	Ano	Ano	příznak Překročení
Ano	Ano	Ano	Ano	úhrada od zdravotní pojišťovny
Ano	Ano	Ano	Ano	číslo žádanky schválené zdravotní pojišťovnou (pole ZCISLOZP dle DR VZP)
Ano	Ano	Ano	Ano	kód diagnózy
Ano	Ano	Ano	Ano	ATC skupina
Ano	Ano	Ano	Ano	kód registrovaného HVLP dle SUKL
Ano	Ano	Ano	Ano	kód přidružené diagnózy
Ano	Ano	Ano	Ano	postup přípravy IPLP

Výdej

Lékař	Lékárník	Pacient	Zdravotní pojišťovna	Atribut
Ano	Ano	Ano	Ano	datum výdeje
Ano	Ano	Ano	Ano	ID dokladu zkrácený
Ano	Ano	Ano	Ano	poznámka k výdeji
Ano	Ano	Ano	Ano	příznak požadavku na upozornění lékaře
Ano	Ano	Ano	Ano	vydávající lékárník – identifikační číslo zařízení PZS (může být prázdné pro výdeje bez úhrady pojišťovnou)
Ne	Ano	Ano	Ano	vydávající lékárník - jméno/jména
Ne	Ano	Ano	Ano	PZS: vydávající lékárník – příjmení
Ano	Ano	Ano	Ano	PZS: vydávající lékárník - část obce
Ano	Ano	Ano	Ano	PZS: vydávající lékárník - číslo evidenční

Ano	Ano	Ano	Ano	PZS: vydávající lékárník - číslo orientační
Ano	Ano	Ano	Ano	PZS: vydávající lékárník - číslo popisné
Ano	Ano	Ano	Ano	PZS: vydávající lékárník - obec
Ano	Ano	Ano	Ano	PZS: vydávající lékárník - okres
Ano	Ano	Ano	Ano	PZS: vydávající lékárník - PSČ
Ano	Ano	Ano	Ano	PZS: vydávající lékárník - ulice
Ano	Ano	Ano	Ano	PZS: vydávající lékárník – DIČ poskytovatele zdravotních služeb
Ano	Ano	Ano	Ano	PZS: vydávající lékárník – IČ poskytovatele zdravotních služeb
Ano	Ano	Ano	Ano	PZS: vydávající lékárník - kód poskytovatele zdravotních služeb
Ano	Ano	Ano	Ano	PZS: vydávající lékárník - název poskytovatele zdravotních služeb

Ano	Ano	Ano	Ano	PZS: vydávající lékárník – telefon poskytovatele zdravotních služeb
Ano	Ano	Ano	Ano	PZS: vydávající lékárník - telefon
Ano	Ano	Ano	Ano	datum a čas změny
Ano	Ano	Ano	Ano	datum a čas založení
Ano	Ano	Ano	Ano	datum a čas zrušení
Ano	Ano	Ano	Ano	důvod zrušení

Položka výdeje

Lékař	Lékárník	Pacient	Zdravotní pojišťovna	Atribut
Ano	Ano	Ano	Ano	název HVLP/neregHVLP/IPLP/INN
Ano	Ano	Ano	Ano	cesta podání HVLP/neregHVLP/IPLP/INN
Ano	Ano	Ano	Ano	forma HVLP/neregHVLP/INN
Ano	Ano	Ano	Ano	množství HVLP/neregHVLP/INN
Ano	Ano	Ano	Ano	síla HVLP/neregHVLP/INN

Ano	Ano	Ano	Ano	počet balení HVLP/neregHVLP/INN
Ano	Ano	Ano	Ano	cena celkem
Ano	Ano	Ano	Ano	cena původce
Ano	Ano	Ano	Ano	datum a čas exspirace
Ano	Ano	Ano	Ano	návod (XXXXX)
Ano	Ano	Ano	Ano	výše úhrady dle lékárny
Ano	Ano	Ano	Ano	započitatelný doplatek dle lékárny/ZP
Ano	Ano	Ano	Ano	ATC skupina neregistrovaného HVLP
Ano	Ano	Ano	Ano	kód HVLP dle SUKL
Ano	Ano	Ano	Ano	ID dokladu výdeje zkrácený
Ano	Ano	Ano	Ano	postup přípravy
Ano	Ano	Ano	Ano	šarže
Ano	Ano	Ano	Ano	EAN

Složka IPLP při výdeji

Lékař	Lékárník	Pacient	Zdravotní pojišťovna	Atribut
Ano	Ano	Ano	Ano	úhrada zdravotní pojišťovny
Ano	Ano	Ano	Ano	jednotka
Ano	Ano	Ano	Ano	množství
Ano	Ano	Ano	Ano	název složky

Ano	Ano	Ano	Ano	kód registrovaného HVLP složky
Ano	Ano	Ano	Ano	kód suroviny složky