Politika Ochrany osobných údajov
v spoločnosti Penta Hospitals International a. s., Digital Park II, Einsteinova 25, Bratislava 851 01, IČO 46 062 513

I.
Účel

1. Penta Hospitals International a. s. pri výkone svojej podnikateľskej činnosti spracúva rôzne údaje a informácie, vrátane určitých druhov Osobných údajov o Dotknutých osobách, ak je takéto spracúvanie nevyhnutné na to, aby Penta Hospitals International a. s. mohla poskytovať svoje služby. Medzi Dotknuté osoby patria napríklad klienti, zamestnanci, dodávatelia a iní obchodní partneri.

2. Táto politika (ďalej ako „Politika“) spolu s na ňu nadväzujúcou dokumentáciou, má za cieľ zabezpečiť, aby získané Osobné údaje boli spracúvané v súlade so všetkými relevantnými všeobecne záväznými právnymi predpismi.

3. Cieľom Politiky je chrániť Osobné údaje najmä klientov a zamestnancov ale aj iných Dotknutých osôb začlenením Ochrany osobných údajov do všetkých aktivít spoločnosti Penta Hospitals International a. s. a zabezpečením súladu Spracúvania osobných údajov so všeobecne záväznými právnymi predpismi.

II.
Rozsah platnosti

1. Táto Politika sa aplikuje na všetky postupy súvisiace so Spracúvaním Osobných údajov v rámci Penta Hospitals International a. s. počnúc od stratégií a obchodných procesov po manuálne Spracúvanie a všetky informačné technológie, ako sú IT systémy, IT infraštruktúra a IT organizácie (ďalej spolu ako „**IT služby**“).

2. Všetky požiadavky tejto Politiky sa vzťahujú aj na IT služby, ktoré sa poskytujú v prostredí Tretích strán.

3. Politika sa aplikuje na všetky Osobné údaje bez ohľadu na ich formu vrátane fyzických archívov a manuálneho Spracúvania Osobných údajov.

4. Politika je vynucovaná výkonným manažmentom Penta Hospitals International a. s..

5. Pojmy a použité skratky

„Audit Ochrany Osobných údajov“ alebo „Audit“- ako je definované v článku 28 a 32 GDPR.

„Dotknutá osoba“ - každá fyzická osoba, ktorej Osobné údaje sa spracúvajú spoločnosťou Penta Hospitals International a. s.

„Ochrana Osobných údajov“- Ochrana Osobných údajov zahŕňa práva a povinnosti jednotlivcov a organizácií v súvislosti so zbieraním, používaním, uchovávaním, zverejnením a poskytnutím Osobných údajov.

„Osobitná kategória Osobných údajov“- údaje, ktoré odhaľujú rasový pôvod alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.

„Osobné údaje“ - sú údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora, ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe

jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.

„Oznámenie o Porušení“- znamená oznámenie nadriadeným orgánom, Prevádzkovateľom alebo Tretím stranám, ako je to uvedené v článku 33 a 34 GDPR.

„Porušenie Ochrany Osobných údajov“ - porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných Osobných údajov alebo inak spracúvaných Osobných údajov, alebo k neoprávnenému prístupu k nim.

„Posúdenie rizík súvisiacich s Ochranou Osobných údajov“ - ako je definované v článku 24 a 35 GDPR .

„Posúdenie vplyvu na Ochranu Osobných údajov“ alebo „DPIA“- ako je definované v článku 35 GDPR.

„Prevádzkovateľ“- každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky Spracúvania Osobných údajov a spracúva Osobné údaje vo vlastnom mene.

„Spracúvanie“- spracovateľská operácia alebo súbor spracovateľských operácií s Osobnými údajmi alebo so súbormi Osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami.

„Sprostredkovateľ“ - každý, kto spracúva Osobné údaje v mene Prevádzkovateľa.

„Špecificky navrhnutá a štandardná Ochrana Osobných údajov“- ako je definované v článku 25 GDPR .

„Tretia krajina“- krajina, ktorá nie je členom Európskej únie a neuzavrela dohodu s Európskou úniou, ktorá obsahuje nariadenia súvisiace so Smernicou 95/46/EEC z 24. októbra 1995 o ochrane fyzických osôb v súvislosti so spracovaním osobných údajov a voľnej výmene týchto údajov – čiže krajiny Európskeho hospodárskeho priestoru (EHP).

„Tretia strana“ - každý, kto nie je Dotknutou osobou, Prevádzkovateľom, Sprostredkovateľom alebo inou fyzickou osobou, ktorá na základe poverenia Prevádzkovateľa alebo Sprostredkovateľa spracúva Osobné údaje.

„Všeobecné nariadenie o ochrane údajov“ alebo „GDPR“ - Nariadenie (EÚ) 2016/679 Európskeho parlamentu a Rady z 27. apríla 2016 o ochrane fyzických osôb v súvislosti so spracovaním Osobných údajov a slobodnom pohybe týchto údajov, ktoré vstupuje do platnosti 24. mája 2018 a je aplikovateľné od 25. mája 2018 v platnom znení.

„Zmluva o spracúvaní Osobných údajov“- je zmluva, ktorý musí byť uzavretá, ak Sprostredkovateľ spracúva Osobné údaje v mene Prevádzkovateľa, ako je to uvedené v článku 28 a 29 GDPR.

„Zodpovedná osoba“ alebo „DPO“- ako je definované v článku 37, 38 a 39 GDPR .

III.
Predmet úpravy

3.1 Princípy a požiadavky

GDPR určuje hlavné zodpovednosti v súvislosti s Ochranou Osobných údajov vrátane princípov pre Spracúvanie. Tieto princípy, povinnosti a zodpovednosti, ktorým sa Penta Hospitals International a. s. musí podriadiť, sú načrtnuté nižšie.

Princípy pre Spracúvanie sú uvedené v GDPR najmä v kapitolách I, II, III a V.

Penta Hospitals International a. s. musí dokumentovať súlad s týmito požiadavkami najmä tak, že uchováva relevantnú dokumentáciu ochrany Osobných údajov.

3.2 Princípy pre Spracúvanie

Penta Hospitals International a. s. pri spracúvaní Osobných údajov v plnej miere podporuje a dodržiava základné princípy GDPR:

1. Osobné údaje sa môžu spracúvať len **zákonným spôsobom**.
2. Osobné údaje sa môžu získavať len na konkrétne určený, výslovne uvedený a oprávnený **účel** a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom (obmedzenie účelu).
3. Spracúvané Osobné údaje musia byť **primerané**, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú (minimalizácia údajov).
4. Spracúvané Osobné údaje musia byť **správne** a podľa potreby aktualizované.
5. Osobné údaje sa nesmú uchovávať dlhšie, než je to nevyhnutné.
6. Osobné údaje sa musia spracúvať v súlade s **právami** Dotknutých osôb
7. Osobné údaje musia byť spracúvané spôsobom, ktorý zaručuje ich primeranú bezpečnosť
8. Osobné údaje sa nesmú prenášať mimo Európsky hospodársky priestor (EHP), ak nie je zabezpečená ich primeraná ochrana

Princípy pre Spracúvanie Osobných údajov sú podrobne opísané v mnohých článkoch GDPR, najmä však v článkoch 5, 6 a 9.

Smernice, formuláre, kontrolné zoznamy a iné dokumenty nadväzujúce na túto Politiku bližšie popisujú, ako majú byť vyššie uvedené princípy primerane a účinne implementované do činností spoločnosti Penta Hospitals International a. s.

3.3 Práva Dotknutej osoby

Osobné údaje Penta Hospitals International a. s. spracúva v súlade s právami Dotknutých osôb, ktoré im priznáva GDPR a ďalšie všeobecne záväzné právne predpisy:

A. Právo na informácie o tom, či sa spracúvajú Osobné údaje, ktoré sa jej týkajú a ďalšie dodatočné informácie s tým súvisiace;
B. Právo na prístup k Osobným údajom, ktoré sa jej týkajú. Dotknutá osoba, ktorá predloží písomnú žiadosť, má právo:
   a. byť informovaná o tom, či sa spracúvajú Osobné údaje, ktoré sa jej týkajú;
   b. byť informovaná o kategóriách spracúvaných Osobných údajov, účele Spracúvania, o príjemcoch alebo o kategórii príjemcov, ktorým boli alebo majú byť jej Osobné údaje poskytnuté ;
   c. získať kópie Osobných údajov, ktoré sa jej týkajú a byť informovaná o zdroji Osobných údajov, ak sa Osobné údaje nezískali od Dotknutej osoby.
C. Právo namietať voči Spracúvaniu, ktoré jej pravdepodobne spôsobí alebo spôsobuje škodu alebo nepríjemnosti;
D. Právo namietať Spracúvanie Osobných údajov, ktoré sa jej týkajú, na účel priameho marketingu vrátane profilovania v rozsahu, v akom súvisí s priamym marketingom;
E. Právo namietať rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní Osobných údajov vrátane profilovania a ktoré má právne účinky, ktoré sa jej týkajú alebo ju obdobne významne ovplyvňujú;
F. Právo za určitých okolností na opravu, obmedzenie Spracúvania, výmaz alebo zničenie Osobných údajov;

G. Právo na náhradu škody spôsobenú jej porušením všeobecne záväzných právnych predpisov pri spracúvaní Osobných údajov.

Práva Dotknutej osoby sú podrobne opísané v mnohých článkoch GDPR, najmä však v článkoch 12-22.

3.4 Dokumentácia a záznamy o spracovateľských činnostiach

GDPR ukladá Prevádzkovateľovi aj Sprostredkovateľovi povinnosť viesť záznamy o spracovateľských činnostiach, ktoré okrem iného obsahujú účel Spracúvania Osobných údajov, kategórie príjemcov a predpokladané lehoty na vymazanie rôznych kategórií Osobných údajov. Záznamy o spracovateľských činnostiach a ďalšia súvisiaca dokumentácia sú ďalej označované len ako „**Dokumentácia**“. Účelom tejto Dokumentácie je podporiť správne nakladanie s Osobnými údajmi a zabezpečiť, že Penta Hospitals International a. s. bude schopná preukázať súlad svojich aktivít a činností s požiadavkami GDPR.

Požiadavky na Dokumentáciu sú spomínané v mnohých článkoch GDPR, najmä však v článku 30.

3.5 Poskytnutie a prenos Osobných údajov do Tretích krajín

Penta Hospitals International a. s. neposkytne žiadne Osobné údaje neoprávneným Tretím stranám, to znamená, že Penta Hospitals International a. s. neposkytne Osobné údaje Tretím stranám, ak to nie je relevantný právny základ. Všetci zamestnanci postupujú veľmi opatrne, keď obdržia požiadavku na poskytnutie Osobných údajov Tretej strane.

Spoločnosť Penta Hospitals International a. s. realizuje prenos Osobných údajov do Tretích krajín len ak je to v súlade s požiadavkami GDPR a len na základe zmluvy zaručujúcej dostatočné bezpečnostné opatrenia.

O poskytnutí Osobných údajov Tretím stranám a ich prenose do Tretích krajín sa hovorí v mnohých článkoch GDPR, najmä však v kapitole V.

3.6 Zmluva o spracúvaní Osobných údajov „DPA“

Ak Osobné údaje spracúva Sprostredkovateľ v mene Prevádzkovateľa, vyžaduje sa Zmluva o spracúvaní Osobných údajov. Zmluva o spracúvaní Osobných údajov sa teda vyžaduje pri všetkých Spracúvaniach, kde spoločnosť Penta Hospitals International a. s. vystupuje ako Sprostredkovateľ alebo kde ako Prevádzkovateľ zapojila Sprostredkovateľa, aby spracúval Osobné údaje v jej mene.

O Zmluvách o Spracúvaní Osobných údajov sa hovorí v mnohých článkoch GDPR, najmä však v článkoch 28 a 29.

3.7 Oznámenie Porušenia Ochrany Osobných údajov

Oznámenie Porušenia Ochrany Osobných údajov podrobne upravuje GDPR v ustanoveniach článku 33 a 34.

Po zistení potenciálneho Porušenia Ochrany Osobných údajov spoločnosť Penta Hospitals International a. s. musí bezodkladne začať vyšetrovanie.

Ak sa vyšetrovaním zistí, že došlo k sprístupneniu, získaniu, použitiu, pozmeneniu alebo poskytnutiu nešifrovaných Osobných údajov v dôsledku Porušenia Ochrany Osobných údajov, bezodkladne **musí byť informovaná DPO a ak nie je ustanovená tak musí byť informovaný priamo štatutárny orgán Penta Hospitals International**

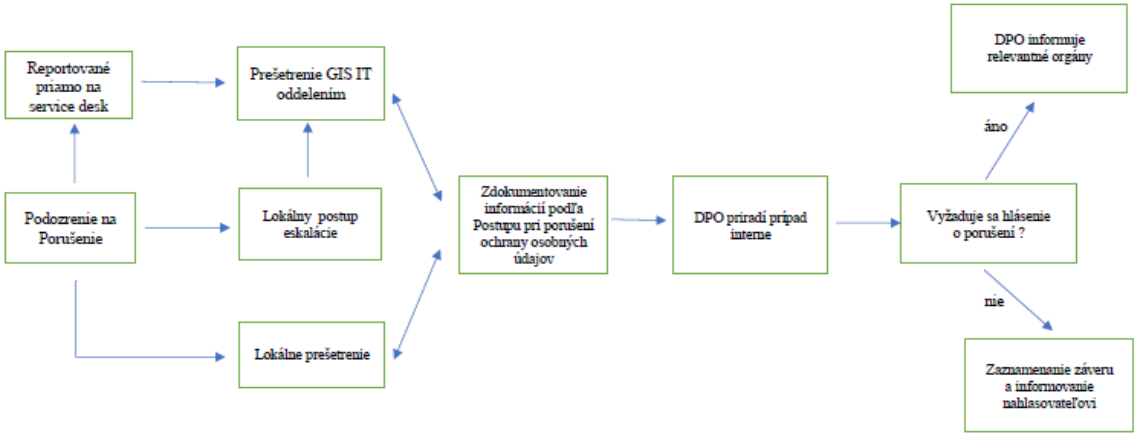
a. s.. Požiadavky na obsah tohto Oznámenia sú predmetom súvisiaceho postupu pri Porušení Ochrany Osobných údajov.

GDPR vyžaduje, aby Oznámenie o Porušení Ochrany Osobných údajov dozorovému orgánu bolo Prevádzkovateľom realizované bez zbytočného odkladu a kde je to možné, **do 72 hodín po tom, ako sa o ňom dozvedel** a to podľa pokynov DPO (ak je ustanovená). Oznámenie musí obsahovať požadované informácie v rozsahu, v akom sú Prevádzkovateľovi známe v čase Oznámenia, ostatné informácie poskytne bezodkladne po tom, čo sa o nich dozvie. Za určitých okolností je potrebné Porušenie Ochrany Osobných údajov oznámiť aj Dotknutým osobám.

Ak je spoločnosť Penta Hospitals International a. s. v postavení Sprostredkovateľa, o Porušení Ochrany Osobných údajov musí byť bez zbytočného odkladu podľa pokynov DPO informovaný aj Prevádzkovateľ.

Oznámenie o Porušení Ochrany Osobných údajov môže byť tiež požiadavkou podľa iných všeobecne záväzných právnych predpisov.

Schematický prehľad procesu súvisiaceho s oznámením Porušenia Ochrany Osobných údajov je nasledovný (ak nie je ustanovená DPO, jej úlohy plní štatutárny orgán):



3.8 Špecificky navrhnutá a štandardná Ochrana Osobných údajov

Špecificky navrhnutá a štandardná Ochrana Osobných údajov je požiadavka GDPR pre implementovanie primeraných technických a organizačných opatrení, aby sa zabezpečilo, že štandardne sa spracúvajú len Osobné údaje, ktoré sú nevyhnutné pre konkrétny účel Spracúvania v súlade s GDPR, čiže **aktívna minimalizácia údajov**, **pseudonymizácia** a iné nástroje na zlepšenie bezpečnosti a Ochrany Osobných údajov.

Používanie špecificky navrhnutej a štandardne určenej Ochrany Osobných údajov je povinné pre Penta Hospitals International a. s., ale samotné opatrenia musia byť založené na Posúdení rizík súvisiacich s Ochranou Osobných údajov.

Penta Hospitals International a. s. musí byť schopná preukázať a zdokumentovať súlad svojich aktivít a činností s touto Politikou a súvisiacimi postupmi ako aj s relevantnými požiadavkami všeobecne záväzných právnych predpisov, preto musí byť dokumentácia ochrany Osobných údajov neustále uchovávaná, kontrolovaná a aktualizovaná.

3.9 Posúdenie rizík súvisiacich s Ochranou Osobných údajov

Na posudzovanie rizík súvisiacich s Ochranou Osobných údajov odkazuje GDPR najmä v ustanoveniach článku 24 a 35.

Produkty, služby a aplikácie Penta Hospitals International a. s., v ktorých sa spracúvajú Osobné údaje, musia byť chránené primeranými technickými a organizačnými opatreniami, aby sa zabezpečilo, že sa štandardne spracovávajú len Osobné údaje, ktoré sú nevyhnutné pre konkrétny účel spracovania. S cieľom zabezpečiť primeranú úroveň technických a organizačných opatrení je nevyhnutné posúdiť riziká súvisiace s Ochranou Osobných údajov. Aby Posúdenie týchto rizík bolo úplné, je nevyhnutné najprv vyhodnotiť pravdepodobnosť a závažnosť negatívneho vplyvu spojeného so spracúvaním Osobných údajov a následne analyzovať charakter, rozsah, kontext a účel Spracúvania, aby sa vyhodnotili zraniteľné stránky IT systémov a operácií ako aj charakter prípadných hrozieb.

Postup pre Posúdenie rizík súvisiacich s Ochranou Osobných údajov musí byť použitý pri identifikácii a vyhodnocovaní potenciálnych rizík nových procesov, nových riešení, nových dodávateľov, partnerov, zákazníkov, atď.

Rovnako musí byť použitý v prípade vysoko rizikového Spracúvania skôr, ako dôjde k výberu nových dodávateľov a Sprostredkovateľov ako súčasť Posúdenia vplyvu na Ochranu Osobných údajov a ako súčasť životného cyklu Ochrany Osobných údajov.

3.10 Posúdenie vplyvu na Ochranu Osobných údajov, DPIA

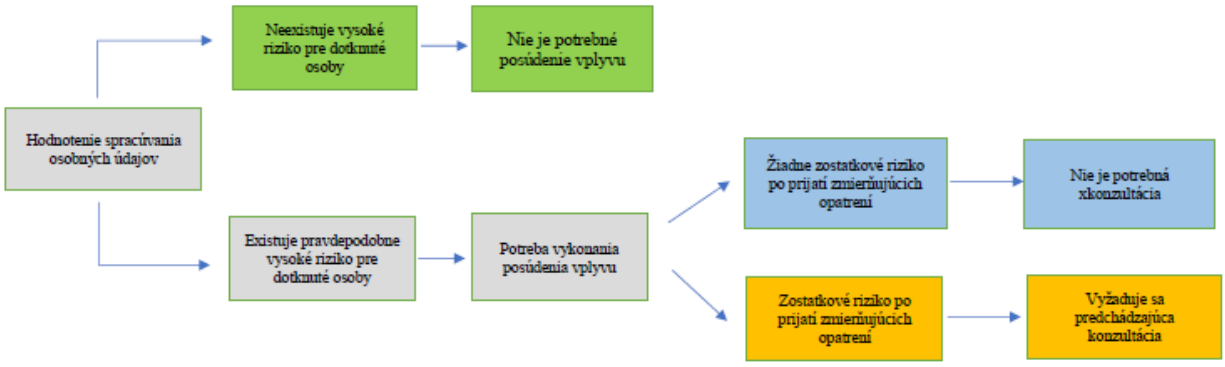
Posudzovanie vplyvu na Ochranu Osobných údajov upravuje GDPR najmä v článku 35 a 36.

DPIA je proces, ktorý má popísať Spracúvanie, vyhodnotiť nevyhnutnosť a proporčnosť Spracúvania a umožniť riešiť riziká pre práva a slobody Dotknutých osôb. Ak typ Spracúvania Osobných údajov, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účel Spracúvania Osobných údajov, môže viesť k vysokému riziku pre práva fyzických osôb, GDPR ukladá Prevádzkovateľovi povinnosť pred spracúvaním Osobných údajov vykonať Posúdenie vplyvu plánovaných spracovateľských operácií na Ochranu Osobných údajov.

DPIA identifikuje najúčinnejší spôsob splnenia povinností súvisiacich s Ochranou Osobných údajov a zabezpečí, že sa implementuje primeraná úroveň Ochrany Osobných údajov pre Dotknuté osoby.

Postup pre vykonávanie DPIA musí byť použitý pri identifikácii a vyhodnocovaní vysoko rizikového Spracúvania.

Prehľad procesu DPIA:



3.11 Audit Ochrany Osobných údajov u Sprostredkovateľov

Audit Ochrany Osobných údajov upravuje GDPR najmä v článku 28 a 32.

Audit Ochrany Osobných údajov sa sústreďuje na overenie súladu Sprostredkovateľov s požiadavkami GDPR a požiadavkami Zmluvy o spracúvaní Osobných údajov. Audit sa vykonáva v určenom rozsahu a podľa systematickej a zdokumentovanej metódy, ako je to uvedené v Smernici pre Audit Ochrany Osobných údajov, s cieľom získať a uchovať relevantnú dokumentáciu o Audite a vyhodnotiť do akej miery sú splnené auditované kritériá.

Ak sa zistí, napríklad Auditom, že Sprostredkovateľ neplní povinnosti súvisiace s Ochranou Osobných údajov, musia byť prijaté nevyhnutné a primerané opatrenia, aby sa tento súlad zabezpečil.

Relevantná dokumentácia o každom Audite sa musí uchovávať.

3.12 Manažment informácií

Ustanovenia súvisiace s požiadavkami pre manažment informácií sú uvedené v mnohých článkoch GDPR, najmä však v článku 5.

GDPR požaduje, aby sa Osobné údaje uchovávali len dovtedy, kým existuje účel ich Spracúvania a kým sú zavedené primerané technické opatrenia. S cieľom dosiahnuť a udržať súlad s GDPR bol pripravený a implementovaný základný postup pre manažment informácií, ktorý je implementovaný v Penta Hospitals International a. s.. Tento postup načrtáva hlavné pravidlá pre ukladanie, uchovávanie a vymazávanie emailov a dokumentov, ktoré obsahujú Osobné údaje.

IV.
Záverečné ustanovenia

Táto Politika Ochrany Osobných údajov je záväzná pre Penta Hospitals International a. s. a všetkých zamestnancov spoločnosti.

Porušenie tejto Politiky bude v súlade s pracovným poriadkom spoločnosti Penta Hospitals International a. s. alebo v súlade s ustanoveniami Zákonníka práce považované za porušenie pracovnej disciplíny zvlášť závažným spôsobom.

Zodpovední riaditelia v Penta Hospitals International a. s. sú povinní zabezpečiť oboznámenie svojich zamestnancov s obsahom tejto Politiky.

Žiaden z interných predpisov Penta Hospitals International a. s. nesmie byť v rozpore s ustanoveniami tejto Politiky. Ustanovenia interných predpisov, ktoré sú v rozpore s ustanoveniami tejto Politiky sa považujú za neplatné.