SHARE FOUNDATION

BIRN
BALKAN INVESTIGATIVE REPORTING NETWORK

Политики и протоколи за медиумите

Заштита на личните податоци и дигитална безбедност

Април 2022

Преводот на македонски јазик е овозможен благодарејќи на проектот Paprer Trail to Better Governance, кој го финансира Австриската развојна агенција (APA), оперативна единица на Австриската развојна соработка, март 2024.

Austrian Development Cooperation

Заштита на личните податоци

Инструкции

Политика за приватност е документ кој треба да се изработи, со цел на публиката на која ѝ е наменет, да ѝ се дадат информации за тоа зошто и на кој начин ракувачот ги користи и обработува личните податоци на тие лица.

Должноста за информирање произлегува од законската обврска на ракувачите, однапред да им ги дадат законски пропишаните информации на лицата чии податоци се собираат. Со цел бараните информации однапред да им бидат достапни на заинтересираните лица, стандардна практика е политиката за приватност да биде јавно објавена на интернет страницата на ракувачот.

Текстот подолу е пример за образец за тоа како ракувачот може да ја опише обработката на личните податоците, што ги собира преку својата интернет страница, во рамките на својата политика за приватност. Насловите на овој пример ги следат задолжителните информации што ракувачот е должен да ги обезбеди, според правилата од GDPR и Закон за заштита на личните податоци.

Во фуснотите се наоѓа објаснување за тоа како овој пример да се прилагоди на потребите на конкретниот ракувач. Во таа смисла, неопходно е во рамките на секоја точка (наслов), да се внесат информации што се релевантни за конкретниот ракувач, вклучително и информации за тоа дека одредени обработки не се вршат. После финализирањето на текстот со потребните информации, фуснотите треба да се избришат.

Доколку операторот не собира никакви лични податоци, се препорачува на веб-страницата да објави известување во кое тоа се констатира.

Примери за конкретни политики за приватност, кои се изработени во согласност со овие препораки, може да се најдат овде или овде.

Политика за приватност

Во понатамошниот текст можете да најдете информации за тоа во кои ситуации, за кои цели и на кој начин доле наведениот ракувач ги обработува личните податоци, а земајќи ги предвид информациите што ракувачите се должни да ги предочат според членовите 13 и 14 од Општата регулатива за заштита на личните податоци на ЕУ (General Data Protection Regulation „GDPR“).

1) Идентитет и податоци за контакт на ракувачот

<Назив>
<Адреса>
<Град, Држава>

2) Контакт податоци на ракувачот, во врска со заштита на личните податоци

<да се наведат податоците за контакт>

3) Цел на обработка, извор на податоци и правна основа за обработка[1]

Цел[2]	***Вид***[3] ***и извор на податоци***[4]	***Правна основа***[5]
<да се наведе целта на обработката на податоците>	<да се наведат начините на собирање и изворите на податоците за оваа цел>	<да се наведе правната основа за обработка на податоците за оваа цел>
<да се наведе целта на обработката на податоците>	<да се наведат начините на собирање и изворите на податоците за оваа цел>	<да се наведе правната основа за обработка на податоците за оваа цел>

или

<во форма на наративен текст, да се наведе/опише посебно секоја цел, информација за тоа на кој начин се собрани податоците за да се исполни таа цел и, доколку е потребно, за какви податоци се работи, како и која е правната основа за секоја конкретна цел>

[1] Информациите во рамките на овој наслов може да се дадат во текстуална или табеларна форма. Во финалниот документ, потребно е да се избрише табелата, односно наративниот текст, во зависност од тоа за која од двете форми се даваат информации во рамките на овој наслов.

[2] Целта може да биде, на пример: давање коментари на веб-страница; пополнување на контакт формулар на веб-страница; учествување во анкети; пријава за билтен; регистрација на веб-страница; донација за ракувачот итн.

[3] Податоците можат да бидат, на пример, од следниот вид: име; е-пошта, адреса; телефон; ИП адреса; содржина на коментари или пораки; број на банкарска сметка итн.

[4] Податоците може да се собираат директно од лицето што податоците му ги дава на ракувачот - на пример, на тој начин што лицето самото ќе ги внесе на веб-страницата, или индиректно - на пример, од јавно достапни извори.

[5] Правна основа за обработка може да биде согласноста на лицето, легитимниот интерес на ракувачот, договорот што ракувачот го има со лицето или исполнувањето на законските обврски на ракувачот. Доколку не сте сигурни, треба, во врска со прашањето за соодветната правна основа, да се консултирате со правник.

4) Примачи на лични податоци[6]

Личните податоци ракувачот ги споделува со <да се наведат примателите на податоци т.е. организациите со кои се споделуваат податоците>.

5) Пренесување на личните податоци во друга држава[7]

Личните податоци се обработуваат во <да се наведат земјите во кои податоците се чуваат/хостираат>.

6) Рок на чување на личните податоци, т.е. критериуми за негово определување[8]

<да се наведе рокот на чување на податоците, т.е. моментот по кој податоците се бришат, при што, доколку има повеќе цели, потребно е да се наведат различните рокови за секоја цел на обработка>.

7) Правата на лицата на кои се однесуваат податоците

Секое лице, на кое се однесуваат податоците што ги обработуваме, има право да побара од ракувачот:

- вистинито и целосно да го информира за обработката на неговите податоци;
- право на увид и/или копија од податоците што се однесуваат на него;
- право на корекција и дополнување на неточните или нецелосните податоци, во секое време;
- право на бришење, кое може да се задоволи во согласност со законските услови, односно кога: личните податоци повеќе не се неопходни за постигнување на целта за која се собрани или на друг начин обработувани; лицето на кое се однесуваат податоците поднело приговор на обработката, врз основа на легитимниот интерес на ракувачот, а не постои друга правна основа за обработката; личните податоци се

[6] Да се внесат примателите на податоците, со кои ракувачот ги споделува податоците (заради подобро разбирање, се препорачува да се наведе и причината поради која податоците се споделуваат). Тоа може да бидат деловни соработници, поврзани стопански друштва или организации, курирски служби, правни и финансиски консултанти, надлежни државни органи итн. Доколку нема примачи со кои се споделуваат личните податоци, во рамките на овој наслов, и тоа треба да се напише.

[7] Да се внесат информации за тоа во кои сè земји се обработуваат податоците. Доколку е потребно, проверете каде е хостирана веб-страницата. Доколку податоците се обработуваат во земји кои не се сметаат за адекватни според меродавните прописи, да се наведе правната основа за пренос на податоците во неадекватните земји.

На пример: Личните податоци се обработуваат во Србија и во Индија. Преносот на податоци во Индија, која не се смета за земја која обезбедува адекватно ниво на заштита на податоците, е регулиран и обезбеден со Стандардни договорни клаузули.

[8] Примери за рокот на чување: личните податоци што се даваат кога се остава коментар, се чуваат трајно, т.е. не се бришат, како ни самите коментари; е-поштата што сте ја дале заради добивање на билтен, се брише кога ќе се одјавите; податоците што ги давате во контакт форма на веб-страница се чуваат најмногу една година од датумот на испраќање на пораката.

незаконски обработувани; личните податоци мора да се избришат со цел извршување на законските обврски на ракувачот;

- право на ограничување на обработката може да се удоволи, доколку се исполнети пропишаниве услови: доколку лицето на кое се однесуваат податоците ја оспорило точноста на личните податоци, а на ракувачот му е потребно време што ќе му овозможи да ја провери нивната точност; доколку обработката е незаконска, а лицето се противи на бришењето и наместо бришење бара ограничување на користењето на податоците; доколку на ракувачот повеќе не му се потребни личните податоци за постигнување на целта на обработката, но лицето ги побарало заради поднесување, остварување или одбрана на правно барање; или доколку лицето веќе поднело приговор на обработката, а во тек е проценка за тоа дали правната основа за обработката од страна на ракувачот, ги надминува интересите на лицето;
- пренос на податоци во машински читлива форма, што постои во случаи кога тоа е применливо, т.е. доколку тоа е технички возможно, бидејќи податоците се машински читливи, и кога правната основа за обработка е согласност на лицето или договорен однос со лицето, на кое се однесуваат податоците.
- право, во секое време да ја повлече својата согласност за обработка на одредени податоци, доколку согласноста е правна основа за обработката.
- Лицето на кое се однесуваат податоците, исто така, има право на приговор, доколку смета дека легитимниот интерес на ракувачот, врз основа на кој се обработуваат податоците, не е оправдан, односно дека ги загрозува правата, слободите и интересите на тоа лице. Во случај да се врши автоматска обработка на личните податоци и на донесувањето на одлука, лицето има право на човечка интервенција, како и право да го изрази својот став за одлуката или да ја оспори одлуката.

8) Право да се поднесе поплака до Повереникот (Агенцијата за заштита на личните податоци, АЗЛП).

Секое лице има право да поднесе поплака против постапувањето на ракувачот до надлежниот орган, чии податоци за контакт се дадени во продолжение:

Агенција за заштита на личните податоци
бул.„Гоце Делчев“бр. 18, (зградата на Македонска радио телевизија МРТВ – кат 14)
Поштенски фах 417
1000 Скопје
https://azlp.mk/kontakt/

9) Постоење на автоматизирано донесување на одлуки, вклучително и профилирање[9]

Ракувачот не врши автоматизирано донесување на одлуки, ниту профилирање, врз основа на лични податоци.

10) Политика за колачиња[10]

<Под овој наслов е даден само пример за тоа како ракувачот, на својата интернет страница, може да го опише користењето на колачиња. Доколку сакате да го искористите текстот подолу, потребно е тој да се прилагоди за употреба за конкретна интернет страница>.

„Колачињата“ се мали податоци што веб-локацијата може да ги испрати до вашиот прелистувач, кои потоа можат да се чуваат на тврдиот диск. Ако сте загрижени за вашата приватноста и за користењето на технологијата „колачиња“, можете во поставките да ја одберете опцијата вашиот прелистувач да ве извести кога ќе добиете „колаче“. Колачињата можат да ви помогнат да бидете поефикасни и да имате корист од функцијата „меморија“, на пример, кога страницата ќе го запомни јазикот на кој сте ја прегледувале нашата страница при последната посета. Колачињата ви овозможуваат да ги зачувате своите преференци, да ги зачувате производите и услугите и да ги прилагодите страниците.

Ракувачот користи колачиња на својата интернет страница, со цел на своите корисници да им обезбеди услуги и функционалност. Можете да ја ограничите или оневозможите употребата на колачиња преку вашиот интернет прелистувач, но без колачиња нема да можете да ја користите сета функционалност на страницата.

---

[9] Медиумите најчесто не вршат профилирање (создавање единствени профили) и автоматизирано донесување на одлуки за правата и интересите на посетителите на нивните интернет страници (донесување на одлуки без човечка интервенција, туку само преку „алгоритми“). Доколку ракувачот сепак го прави тоа, потребно е јасно и разбирливо да се објаснат целите и начините на кои се врши таквата обработка.

[10] Доколку користите колачиња кои можат да доведат до директна или индиректна идентификација на одредени корисници на вашата интернет страница (преку кој било единствен идентификатор), употребата на таквите колачиња, исто така, се смета за обработка на лични податоци.

Во тој случај, прво треба да утврдите дали има колачиња за кои имате легитимен интерес да ги користите (како што се строго неопходните колачиња), што, во тој случај, е правна основа за обработка на податоците.

Сите други колачиња може да се користат само врз основа на согласноста на посетителите на страницата.

Во тој случај е потребно и препорачливо да овозможите поп-ап опција, со која посетителите на страницата ќе имаат можност да ги одбијат сите колачиња што не можат да се оправдаат со легитимен интерес, како што се аналитичките, маркетиншките и колачињата од трета страна.

Практиките во кои посетителот на страницата се информира само дека со користење на страницата ги прифаќа сите колачиња, без разлика на нивниот вид и намена, не се во согласност со стандардите на GDPR.

Постојат различни видови на колачиња, а според критериумот, кој ги поставува колачињата на интернет страницата, разликуваме:

- колачиња од прва страна (first party cookies) - колачиња што ги поставува ракувачот кога ја користите нашата интернет страница, и
- колачиња од трета страна (third party cookies) – колачиња што ги поставува некоја друга организација, кога ја користите нашата интернет страница (некои веб-страници на нашата страница, исто така, може да содржат и содржини од други страници, кои може да поставуваат сопствени колачиња).

Што се однесува до намената, на интернет страницата ги користиме следниве видови колачиња:

- Строго неопходни колачиња - овие колачиња се неопходни за управување со статусот на вашата врска.
- Функционални колачиња - овие колачиња ѝ овозможуваат на веб-страницата да ги запомни вашите претходни дејства, за да ви обезбеди напредна функционалност.
- Аналитички колачиња - овие колачиња ни овозможуваат да собираме податоци за вашето користење на веб-страницата, со цел подобрување на нејзините перформанси и дизајн. За да ги оневозможите колачињата на Гугл Аналитика, преземете го и инсталирајте го овој додаток.
- Маркетинг колачиња - овие колачиња се користат за собирање на различни информации за вашата посета на нашата страница, како што се информации за содржината што сте ја гледале, врските што сте ги следеле, вашиот прелистувач, уред или ИП адреса.

Дигитална безбедност

Интерни безбедносни политики

Дигиталната безбедност е од клучно значење за медиумските организации и за луѓето кои ги сочинуваат, односно за новинарите и другите вработени, како и за изворите со кои новинарите доаѓаат во контакт при истражувањата. За да биде користењето на технологијата при извршувањето на нивната работа што побезбедно, медиумите треба да усвојат соодветни политики и процедури, кои ќе им помогнат во тоа. Во случај на технички инциденти, како што се, на пример, нападите на интернет страниците на медиумите или преземањето на сметката, овие политики може да помогнат да се спречи или барем да се минимизира штетата врз ресурсите на организацијата.

Во зависност од капацитетот и ресурсите на организацијата, креирањето на политиките за интерна безбедност, вклучува учество на менаџментот, на уредниците, на членовите на тимот задолжени за ИТ, како и на новинарите и другите вработени, кои поседуваат понапредни технички вештини, што можат да им ги пренесат на другите. Обуката и едукацијата на вработените се важни, за да може процедурите и политиките да се применат, без да се нарушат редовните работни процеси.

Секој интерен документ од областа на дигиталната безбедност, треба да биде прилагоден на реалните потреби и можности на организацијата, на начин да не биде преобемен, туку прецизен и напишан на разбирлив јазик. Интерните политики мора да им бидат достапни во електронска форма само за членовите на тимот, односно не и јавно. За овие цели, на пример, може да се користат платформи за внатрешна комуникација (на пр. Mattermost, Rocket.Chat, Element) за да можат вработените, во случај на недоумица или работа надвор од просториите на организацијата, да имаат пристап до документацијата и да можат да се консултираат со колегите или лицата одговорни за надзор над примената на политиките (на пример, со уредниците).

Примери за интерни документи се **политиката за лозинки, политиката за користење на службена е-пошта и придружни сметки**, како и **безбедносниот план**.

Политика за лозинки

Инструкции

Целта на овој документ е да им помогне на организациите да креираат единствена политика за користење и управување со лозинки, за да се обезбедат предвидливост и јасни процедури. Политиката за лозинки ѝ обебедува на организацијата и на нејзините членови безбедно креирање, користење, складирање и менување на лозинките, кои претставуваат основни механизми за автентикација, односно заштита на организациските ресурси од неовластен пристап.

_____ (назив на организацијата)

Политика за лозинки

1. Оваа политика се применува на лозинките (passwords), што се користат за заштита на сметките, уредите, документите, базите на податоци и на другите ресурси, со кои управува _____ (назив на организацијата).
2. Една лозинка не смее да се користи за заштита на повеќе различни ресурси. Лозинките не смеат да бидат јавно прикажани, ниту споделени со неавторизирани лица.
3. Доколку постои техничка можност, потребно е да се воведе двојна верификација при пријавувањето (2-step verification) на секој ресурс, со кој управува _____ (назив на организацијата).
4. Промена на сите лозинки за ресурсите со кои управува _____ (назив на организацијата), се врши на период од _____ месеци.
5. Лозинките мора да имаат најмалку 15 знаци, мора да содржат специјални знаци (на пр. интерпункциски знаци), големи букви, мали букви и бројки. Лозинките не смеат да содржат лични податоци на вработените (на пр. имиња, презимиња, датуми на раѓање, телефонски броеви, адреси на живеење) или лица блиски до нив (на пр. членови на нивното потесно семејство).
6. За особено чувствителни ресурси (на пример, бази на податоци што содржат податоци од особено чувствителна природа: жртви на насилство, здравствена состојба, сексуална ориентација итн.), неопходно е да се воведат заштитни фрази (passphrases), што се состојат од низа случајно избрани зборови, во комбинација со други задолжителни елементи како за лозинките од точка 5 на оваа политика. Безбедносните фрази мора да имаат најмалку 20 знаци.
7. Лицето во организацијата одговорно за администрирање на лозинки е _____ (име и презиме, работно место).
8. После доделувањето на лозинки за сметките што се користат за работа и активности на _____ (назив на организацијата), како што се, да кажеме, службените сметки за е-пошта, вработените се обврзани да ја сменат дадената лозинка, во согласност со оваа политика, веднаш откако ќе ја добијат од надлежното лице кое ја креирало сметката (на пр. техничкиот администратор) и му ја доделило на вработениот. Новите лозинки мора да се генерираат и складираат во управувач со лозинки.
9. Лозинките и безбедносните фрази се чуваат во специјални апликации, наменети исклучиво за управување со лозинки (на пр. KeePass, KeePassXC), кои ја чуваат базата на лозинки на локална меморија на уредот. Не е дозволено зачувување на лозинки во интернет прелистувачите (internet browsers) и на страниците за онлајн чување на лозинки.

10. При секоја измена на лозинките и безбедносните фрази (додавање на нови или менување на старите), се прави резервна копија на базата на лозинки, која се чува на екстерна меморија (на пр. надворешен тврд диск, УСБ флеш меморија) и задолжително, во името на датотеката, се наведува и датумот кога таа е направена.
11. Во случај некој од вработените да забележи или да се сомнева дека некој ресурс со кој управува _____ (назив на организацијата) е компромитиран, тој веднаш за тоа ќе го извести својот претпоставен и ќе ја смени лозинката или безбедносната фраза за тој ресурс, и доколку станува збор за ресурс што се користи заеднички, ќе го извести лицето кое во организацијата е одговорно за администрирање на лозинките.
12. Оваа политика стапува на сила ____ ден/а од денот на нејзиното донесување.

Датум:_____ Овластено лице на организацијата:_____
Место:_____

Политика за користење на е-пошта и придружни сметки

Инструкции

Со помош на овој документ, организациите можат да креираат единствена политика за користење и управување на службените сметки на е-поштата и со нив поврзаните сметки (т.е. комплетните пакети на услуги за продуктивност, што ги нудат давателите на услуги, како што се Гугл или Мајкрософт), за да биде јасно за какви цели може да се користат, кому се доделуваат, како се постапува при заминување на членовите на тимот од организацијата и слично. Политиката за сметки им овозможува на организациите и нивните членови, со сметките во сопственост на организацијата, да управуваат на начин кој ги намалува можните ризици во поглед на дигиталната безбедност и да ги користат во согласност со пропишаните цели.

Назив и адреса на организацијата

Политика за користење на е-поштата и на придружните сметки _____ (назив на организацијата)

Оваа политика ги содржи условите за користење на е-поштата и придружните сметки на интернет домените во сопственост на _____, и тоа: _____ (да се наведат домените, на пр. organizacija.rs) (во натамошниот текст: домени _____).

1. Е-поштата и придружните сметки, креирани за потребите на работата, практиката и волонтирањето во _____ се во сопственост на _____.
2. _____ управува со сметките и ги издава на користење на лицата кои се во работен однос во _____, на лицата на практикантска работа и лицата кои волонтираат.
3. Лицето на кое му е доделена сметка за е-пошта, ја користи сметката и _____ нема увид во содржината на таа сметка или на нејзините придружни делови (зачувување во облак, колаборативни документи итн.).
4. Сметките на домените _____ се користат исклучиво за цели што ќе ги одреди _____.
5. Во случај на прекин на односот помеѓу _____ и лицето на кое му е издадена сметката, сопственоста на сметката останува кај _____.
6. _____ ќе остави рок од 30 дена од денот на раскинување на односот, за да може лицето на кое му е доделена сметка, од неа да ја собере сета содржина што мисли дека ќе му биде потребна.
7. По истекот на 30 дена од раскинувањето на односот, сметката ќе биде избришана, а копијата на содржината архивирана за цели на _____.
8. Политиката стапува на сила на датумот на нејзино донесување.
9. Лицата на кои им се доделени сметки, ќе бидат известени за секоја идна промена на оваа политика.

Место и датум,

Одговорно лице

_____

Безбедносен план

Инструкции

Безбедносниот план има за цел да им помогне на организациите да креираат превентивни и реактивни мерки во врска со техничките инциденти, да ги разгледаат можните ризици и закани за техничката инфраструктура на организацијата, да ги пропишат процедурите и чекорите во случај на соочување со различни видови на технички инциденти итн. Иако не е можно да се предвиди сценариото на секој поединечен технички напад, поседувањето на безбедносен план може да ја спречи или да ја намали штетата и да помогне да се изврши санација.

При изработката на безбедносниот план, обрнете внимание на следново:

Цели: Поставете реална примарна цел или повеќе секундарни цели, за пропишаните мерки да можат навистина да бидат применети во насока на постигнување на дадените цели.

Закани и ризици: размислете за можните сценарија за загрозување на дигиталната безбедност на вашата организација и на нејзините членови. Тоа ќе ви помогне попрецизно да ги идентификувате можните закани и ризици по дигиталната безбедност и подобро да се подготвите за справување со нив.

Превентивни чекори: наведете реални чекори што можете да ги преземете во врска со заштитата на полето на дигиталната безбедност, земајќи ги предвид заканите, ризиците и капацитетите на самата организација (технички, организациски и кадровски).

Чекори во случај на инцидент: разгледајте ги можните сценарија во случај на инцидент (на пр. неовластено преземање на сметките на социјалните мрежи) и дефинирајте ги неопходните чекори во дадената ситуација. Иако не е реално да се предвидат сите сценарија, изберете неколку за кои мислите дека е најреално да се случат или кои веќе и се случиле на вашата организација.

Препорачани уреди и опрема: направете листа на хардверски и софтверски решенија, кои имаат добра репутација и рецензии и кои се препорачуваат од експертската заедница. Имајте ги на ум капацитетите на организацијата, а доколку не сте сигурни што најмногу би им одговарало на вашите потреби, побарајте совет од надвор.

Примена на интерни процедури: опишете ја конкретно примената на вашите безбедносни процедури, во повеќе примери на инциденти, за кои сметате дека е најреално да се случат или кои претходно сте ги искусиле во организацијата.

Безбедносен план

ЦЕЛ	**Да се унапреди дигиталната безбедност на организацијата како целина и безбедноста на нејзините поединечни членови**
ЗАКАНИ И РИЗИЦИ	• Компромитирање на лични податоци и доверливи информации (документи, преписки...). • Компромитирање на техничката инфраструктура и ресурси на организацијата. • Губење на контрола врз инфраструктурата и податоците.
ПРЕВЕНТИВНИ ЧЕКОРИ	• Пристапот до инфраструктурата и до ресурсите на организацијата (сервери, мрежна опрема, сметки на социјални мрежи, админ панели на интернет страници...) да им биде овозможен само на одредени лица и тој треба да биде заштитен со силни лозинки, кои се чуваат во посебни апликации за таа намена (password managers, на пример: KeePass). • Усвојување на политика за лозинки на организацијата. • Двојна автентикација (2-step authentication) вклучена на сите кориснички сметки што ја поддржуваат. • Особено чувствителните податоци (на пр. информации за жртви на сексуално насилство) да се чуваат енкриптирани, на посебни уреди, кои не се користат во секојдневната работа. • Уредите на вработените да се заштитат со лозинки/пин кодови. • Редовно правење на резервни копии (backup) на локалните уреди (на пр. екстерни тврди дискови) и/или онлајн (на серверот на организацијата или на облак услугите, на пр. Dropbox, Google Drive, OneDrive...). **Меѓутоа, особено чувствителни податоци за личности и другите доверливи информации, не треба да се чуваат на облак сервисите.** • За размена на доверливи информации, да се користат енкриптирани мејлови (PGP) и чет апликации (Signal).

ЧЕКОРИ ВО СЛУЧАЈ НА ИНЦИДЕНТ	• Што побрзо да се известат надлежните колеги (администраторите задолжени за техничка инфраструктура во организацијата) и техничката поддршка (на пр. хостинг компанија) и да се следат нивните инструкции. • Да се соберат сите достапни инфармации за инцидентот (време, место, активности за време на инцидентот, ИП адреси, логови, скриншотови, последни исправни конфигурации...) за да се утврди штетата и последиците. • Да се известат посебните/секторски тимови за реакција, во случај на сајбер инцидент: • **SHARE CERT**, чиј основач е Фондацијата SHARE, е прв посебен центар за заштита на информациските системи онлајн и на граѓанските медиуми и превенција од ризик во сајбер опкружувањето: • Адреса: Капетан Мишина 6а, канцеларија 31, Белград • Е-пошта: info@sharecert.rs, emergency@sharecert.rs • Веб-страница: sharecert.rs • Телефон: 064 089 7067 • Да се пријави инцидентот кај надлежните државни органи: • **МВР на Република Северна Македонија, Сектор за компјутерски криминал и дигитална форензика (при Бирото за јавна безбедност):** • Адреса: ул. „Димче Мирчев“ бр.9, Скопје • Е-пошта: kontakt@moi.gov.mk • Веб-страница: mvr.gov.mk • **Основно јавно обвинителство за гонење на организиран криминал и корупција** • Адреса: Кеј „Димитар Влахов“ бр. бб Скопје Е-пошта: jorm@jorm.org.mk • Веб-страница: jorm.gov.mk • Телефон: +389 76 304-872

	• **Доколку се компромитирани личните податоци, потребно е да се извести (Агенцијата за заштита на личните податоци):** • Адреса: бул.„Гоце Делчев“ бр. 18 Скопје • Е-пошта: azlp.mk/kontakt • Веб-страница: azlp.mk • Да се провери последната достапна верзија на податоците/конфигурацијата на системот, со цел да се обидете да ги вратите во претходна состојба и заради реконструкција на нападот.
ПРЕПОРАЧАНИ УРЕДИ И ОПРЕМА	• Мобилни телоефони со инсталирани енкриптирани чет апликации (Signal). • Компјутери: инсталиран и редовно ажуриран антивирусен софтвер, како и сите други софтвери што се користат. • Компјутери: инсталиран менаџер за лозинки (на пр. KeePass, KeePassXC). • Компјутери: инсталиран софтвер за енкрипција на тврдиот диск (VeraCrypt). • Креирани ПГП клучеви за е-поштата на вработените и инсталиран соодветен софтвер (на пр. Thunderbird, Gpg4Win, Mailvelope). • Прелистувач: Mozilla Firefox, инсталирани додатоци (HTTPS Everywhere, Privacy Badger, uBlock Origin, minerBlock, Facebook Container) или Brave на кој можат да се инсталираат верзии на додатоци за Гугл хром (Google Chrome). • На уредите инсталиран доверлив ВПН (VPN), (на пр. Mullvad, ProtonVPN) и Tor Browser.

ПРИМЕНА НА ИНТЕРНИ ПРОЦЕДУРИ (ПРИМЕР)	Од страна на вработените е забележано дека веб-страницата на организацијата е недостапна или дека страницата тешко се вчитува. 1. Да се провери достапноста на страницата на сервисот „Down For Everyone Or Just Me” (https://downforeveryoneorjustme.com/) и интернет конекцијата. 2. Да се изврши скенирање со антивирусниот софтвер на сите компјутери и уреди. 3. Доколку се утврди дека не се работи за технички проблем, вработениот, лично или преку сигурен канал за комуникација (Signal чет, енкриптирана е-пошта порака), го известува техничкиот администратор на организацијата. 4. Администраторот, во соработка со техничката поддршка, врши проверка на инфраструктурата и, доколку се утврди дека дошло до невообичаен сообраќај, до неовластен пристап или до друга повреда на интегритетот на информацискиот систем, врши прибирање на дигитални докази. 5. Следи обид за враќање на податоците/враќање на функционалноста, со помош на резервни копии и/или последни добри конфигурации. 6. Следи утврдување на видот на нападот и правна квалификација, известување на надлежните органи и подготвување на поднесоци (на пр. кривични пријави) во соработка со посебните/секторски тимови (на пр. SHARE CERT)