URZĄD OCHRONY DANYCH OSOBOWYCH

ЯК КОРИСТУВАТИСЯ ПРАВАМИ, ГАРАНТОВАНИМИ ЗАГАЛЬНИМ РЕГЛАМЕНТОМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ (RODO)?

Загальний регламент про захист персональних даних (RODO) — це акт, який безпосередньо застосовується в усіх державах-членах Європейського Союзу, в єдиному порядку регулюючи права громадян та обов'язки адміністраторів даних.

Персональні дані – це інформація, яка підтверджує та ідентифікує Вашу особу - це ім'я, прізвище, адреса проживання, номер телефону, адреса електронної пошти або дані про місцезнаходження.

Обробка персональних даних — це всі види діяльності, які використовують персональні дані, наприклад збір, збереження, упорядкування, зберігання, перегляд, використання або обмін.

Загальний регламент про захист персональних даних (RODO) надає фізичним особам багато прав, які дозволяють краще контролювати персональні дані.

Управління захисту персональних даних підготувало 10 порад щодо використання прав, гарантованих Загальним регламентом про захист персональних даних (RODO).

Ви маєте право знати, що станеться з вашими даними

Ви повинні знати, хто, на якій підставі та з якою метою обробляє ваші персональні дані. Компанія чи установа, яка володіє Вашими даними, зобов'язана повідомити Вас про це, також зобов'язана вказати, які права надає вам RODO. Вам має бути надано доступ до ваших персональних даних, право виправляти їх, видаляти, обмежувати обробку даних, передавати, висловлювати заперечення або отримувати інформацію про автоматизоване прийняття рішень, включаючи профілювання. При виконанні інформаційних зобов'язань адміністратор також повинен вказати, як довго він зберігатиме Ваші дані, та надати контактні дані Інспектора захисту персональних даних (IOD), якщо такий був призначений.

Вам надано дозвіл в будь-який час відкликати свою згоду на обробку даних

Якщо підставою для обробки Ваших даних є Ваша згода, виявлена свідомо та добровільно, Вам надано право відкликати її в будь-який час, і це не повинно спричинити жодних негативних наслідків (наприклад, збільшення плати за послуги понад стандартну суму). Пам'ятайте, що відкликати згоду має бути так само легко, як і надати її.

Про обробку персональних даних Ви повинні бути поінформовані у зрозумілий для вас спосіб

Вся надана Вам інформація, стосовно обробки персональних даних, має бути сформульована в чіткій, простій та зрозумілій для Вас формі. Це також стосується інформаційних повідомлень, пов'язаних із використанням інтернет-сервісів або мобільних додатків. Якщо Ви їх не розумієте або інформація є недостатньо зрозумілою для Вас, зверніться до адміністратора за додатковими поясненнями у цій справі. У Польщі офіційною мовою являється польська, тому усі повідомлення будуть надіслані цією мовою, але їх також можуть додатково перекладати на інші мови.

Ви маєте право бути забутим (видалення даних), але не завжди

Хоча RODO надає право бути забутим (видалення даних), пам'ятайте, що воно не є абсолютним. Ви можете подати запит на його виконання, наприклад, коли дані стали непотрібними для досягнення передбачуваних цілей, дані були оброблені незаконно або Ви відкликали свою згоду і немає інших причин для легалізації їх використання.

Однак пам'ятайте, що не у всіх випадках Вам надано право на видалення даних Це має місце, наприклад, коли певна організація (наприклад, школа, громадська установа чи клініка) змушена використовувати ваші дані для виконання покладених на неї юридичних зобов'язань.

Ви маєте право бути поінформованими про порушення в обробці ваших даних

Витік даних, втрата або розголошення стороннім особам, нажаль, трапляється, і якщо це становить для Вас серйозну загрозу, не дивуйтеся, що адміністратор повідомить Вас про це – це його прямий обов'язок. Тому дотримуйтесь його інструкцій, завдяки яким Ви зможете мінімізувати загрозу. Іноді, наприклад, зміна пароля в Інтернет-системі або блокування документів дозволить Вам захистити свої дані і уникнути, крадіжки особистих даних і пов'язаних з цим наслідків, наприклад, отримання кредиту від вашого імені.

Якщо у Вас виникли сумніви, зверніться до адміністратора або призначеного ним інспектора із захисту персональних даних, який має допомогти Вам у такій ситуації.

Якщо Ви не погоджуєтесь на обробку даних - маркетинг повинен бути припиненим

Якщо Ваші дані використовуються в маркетингових цілях, тобто для того, щоб суб'єкт міг представити вам пропозицію товарів або послуг, Ви маєте право відмовитися від даних послуг в будь-який час.У випадку відмови обробки даних, ваші дані більше не можуть використовуватися в таких цілях.

Захистіть дітей від недобросовісних дій

Якщо Ви являєтесь батьком або опікуном особи, яка не досягла 16 років, пам'ятайте, що коли вона користується т.зв. інформаційними послугами суспільства (наданих в електронному вигляді), тобто соціальні мережі, програми чи ігри, то Ви виражаєте згоду на обробку персональних даних неповнолітньої особи. Це важливо, оскільки діти часто менше усвідомлюють ризики та наслідки обробки їхніх персональних даних. RODO вказує, що їм слід надавати особливий захист, коли їхні дані використовуються в маркетингових цілях або при створенні особистих профілів. Зверніть увагу на те, чи повідомлення, які їм надсилає адміністратор, написані в зрозумілій для них формі.

По-перше, вимагайте від адміністратора реалізувати Ваші права

Якщо Ви вважаєте, що хтось неправильно обробляє ваші дані, спочатку зв'яжіться з адміністратором (або призначеним ним інспектором IOD) і попросіть пояснення або виконання Вашого запиту, наприклад, спростування даних, реєстрацію скарги, видалення даних.

Ви можете вимагати відшкодування збитків у суді

Пам'ятайте! Якщо субєкт, який володіє Вашими даними, використовує їх всупереч RODO, і в результаті цього Ви зазнали матеріальної чи моральної шкоди, можете вимагати від нього відшкодування, ініціюючи судовий розгляд. Ви маєте право на це, незалежно від того, чи збираєтеся Ви подавати скаргу до Голови Управління захисту персональних даних.

ЯК ПОДАТИ СКАРГУ ДО ГОЛОВИ УПРАВЛІННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ (UODO)?

Кожен, хто вважає, що його права у сфері захисту персональних даних прушено, може подати скаргу на адміністратора до Голови Управління захисту персональних даних. Скарги можуть бути подані в письмовій або електронній формі. Скарга направляється в електронну скриньку Голови Управління, після заповнення ФОРМУЛЯРУ у вигляді «Загального листа до державної установи», доступного на порталі ePUAP2.

Пам’ятайте, що кожна скарга повинна містити:
- Ваше ім'я,прізвище та адресу проживання;
- зазначення суб'єкта, на який ви подаєте скаргу (назву / ім'я та прізвище та адресу зареєстрованого офісу / місця проживання);
- детальний опис порушення;
- Ваш запит – яких дій Ви очікуєте від Управління захисту персональних даних (наприклад, видалення даних, виконання інформаційних зобов’язань, виправлення даних, обмеження обробки даних тощо).
- підпис;

Не забудьте додати докази, що підтверджують неправильну роботу адміністратора (наприклад, листування з адміністратором, договори, сертифікати),це полегшить оцінку ситуації працівникам Управління.

Скарги, в яких не вказано Вашого прізвища, імені та адреси, залишаються без розгляду через відсутність контакту з позивачем.

ЯК ЗАХИСТИТИ ПЕРСОНАЛЬНІ ДАНІ?

Персональні дані дуже цінні, завдяки ним Ви можете отримати доступ до багатьох товарів та послуг. Але їх також можуть використовувати в цілях маркетингу та продажу або, на жаль, у злочинних цілях. Для кращого захисту персональних даних кожної людини та їх безпечної обробки, в Європейському Союзі існують спеціальні правила, створені з метою захисту даних – це Загальний регламент захисту персональних даних (RODO).

Управління захисту персональних даних надає кілька найважливіших порад щодо захисту Ваших персональних даних.

1. Будьте уважні, звертайте увагу на те яку інформацію про себе ви подаєте в інтернеті, а також, кому подаєте цю інформацію

Буває, що Ви надмірно ділитеся інформацією про себе в інтернеті, а в соцмережах ділитеся інформацією про себе, свій майновий стан, місце роботи, події у вашому повсякденному житті, ділитеся місцем розташування, завантажуєте фотографії. Завдяки цьому Інтернет стає джерелом знань про Ваші погляди, поведінку як покупця та інтереси. Ці дані дозволяють відділам маркетингу різних компаній, коригувати та адресувати під Ваші запити свої пропозиції. Таку інформацію також можуть використовувати шахраї у злочинних цілях, собливо якщо Ваш профіль є повністю загальнодоступним, у такому випадку Ви можете бути піддані використанню Ваших даних без Вашого відома та згоди всупереч цілям, для яких Ви надали ці дані.

2. Не залишайте документи під заставу
Згідно з законом, затримання під заставу ID-картки або паспорта без законної на те підстави карається законом. Втрата посвідчення особи або паспорту може привести до того, що цей документ буде використано без Вашого відома чи вираженої згоди, що, у свою чергу, створює ризик крадіжки особистих даних.

3. Не дозволяйте робити копії
Як правило, не варто погоджуватися на копіювання документів, що посвідчують особу. Лише в певних ситуаціях це допустимо, у випадках, коли це дозволяє закон. Коли адміністратор вимагає копію, наприклад, Вашого паспорту, попросіть його вказати Вам правову підставу, яка накладає на нього обов'язок це зробити.

В інших випадках, наприклад, оренда обладнання, ця практика продовжує наражати нас на ті самі небезпеки, тому не погоджуємося на це.

4. Не передавайте свої дані по телефону
Уникайте передачі даних по телефону, особливо коли не Ви ініціюєте дзвінок, а хтось телефонує вам. Дистанційний обмін даними є ризикованим, оскільки невідомо, кому насправді передаються дані.

Переконайтеся, кому насправді передаєте свої дані під час телефонної розмови, і, якщо необхідно, зверифікуйте номер, наприклад, передзвоніть і перевірте, чи даний номер і особа насправді представляють субєкт, на який вони посилаються.

5. Будьте обережні при заповненні різноманітних формулярів, у яких ви подаєте свої дані
Будьте обережні при заповненні та підписанні різних видів анкет, бланків чи договорів. Подумайте, чи дійсно Ви хочете створити картку лояльності в магазині для отримання знижок або додаткових акцій. У таких ситуаціях Ви надаєте магазинам своє ім'я,прізвище, адресу, дату народження, адресу електронної пошти, номер телефону, а натомість отримуєте акції, ваучери на знижки та додаткові подарунки при покупці.

Слід пам'ятати, що адміністратор повинен виконати перед Вами своє інформаційне зобов'язання, тобто надати Вам необхідну інформацію про себе, надавши, зокрема, назву, контактні дані та контактні дані інспектора з персональних даних (якщо він призначений), вказати для чого, з якою метою та на якій правовій основі вони обробляють дані.

6. Уникайте надання надмірної кількості даних
Не надавайте жодних даних, які дозволяють повну ідентифікацію, якщо це не є необхідним в даній ситуації, надмірних даних. Якщо Вам потрібно скористатися певною послугою, надайте лише ті дані, які необхідні для її виконання – уважно подумайте про надання тих, надання яких позначено як необов'язкове.

7. Я погоджуюсь...
Перш ніж підтвердити всі згоди, які дозволяють обробку Ваших персональних даних, з'ясуйте, яких даних вони стосуються. Зверніть увагу,чи у формі згоди вони не вибрані за замовчуванням.

Також уважно прочитайте, на що поширюються положення про згоду. Якщо Ви сумніваєтеся, ставте запитання адміністраторам. Вони повинні повідомити Вас про період, протягом якого дані будуть оброблятися, і про Ваші права, включаючи доступ до даних, виправлення, видалення або заперечення щодо обробки, а також про те, чи будуть Ваші дані передані комусь іншому (іншим одержувачам).

Пам'ятайте, що часто Ви надаєте згоду на використання даних у маркетингових цілях не лише адміністраторам, а й його діловим партнерам. Якщо можете, перевірте, хто вони і які компанії.

Згоди на маркетинг третьої сторони мають бути необов'язковими, і Вам має бути надано право вибору давати таку згоду чи ні.

Адміністратор повинен переконатися, що можливість відкликання згоди є такою ж простою, як і її надання, і Ви повинні бути поінформовані про право відкликати згоду до того, як Ви надасте її.

8. Не викидайте дані в сміття, поки вони не знищені

Будь-які документи з Вашими даними - це ще одне джерело інформації про Вас, особливо коли вони містять багато різної персональної інформації, що дозволяє робити висновки про Вашу особу. Тому перед тим, як викинути документи в смітник, їх необхідно знищити (наприклад, фактури, рахунки), нотатки, наклейки на упаковках кореспонденції або доставлених товарів, таким чином, щоб вони не підлягали відтворенню персональних даних, що містяться на них.

9. Видаляйте назавжди дані з носія

Багато даних про Вас може зберігатись на Ваших старих жорстких дисках, картах пам'яті, флешках чи інших носіях. Зверніть увагу, що все більше інформації про Вас зберігається на комп'ютерах, смартфонах, фотоапаратах і планшетах. Перш ніж позбутися таких пристроїв або носіїв, назавжди видаліть з них дані. Однак простого їх видалення буде недостатньо, оскільки можна відновити багато даних, тому перед тим, як викинути чи продати носій, видаліть з нього дані, використовуючи відповідне програмне забезпечення. Варто також відновити пристрій до заводських налаштувань, щоб він не пам'ятав логіни та паролі для різних сервісів і додатків, якими ви користувалися, особливо тих, якими Ви досі користуєтеся.

10. Використовуйте програми, що захищають мобільні пристрої

Використовуйте програмне забезпечення, яке захищає мобільні пристрої, смартфон або комп'ютер, від небажаних дій ззовні, наприклад, шкідливого програмного забезпечення. Крім популярних антивірусних програм, захищають від зовнішнього втручання, т. зв брандмауер (firewall). Поточні оновлення важливі. Зловмисне програмне забезпечення, від якого ці інструменти захищають нас, створюється щодня. Тому без актуальної бази вірусів та бази шкідливих програм антивірусна програма не буде повноцінно виконувати свою роль.

11. Уникайте громадських точок доступу

Уникайте «відкритих» точок доступу, доступних для всіх у людних місцях. Якщо Ви використовуєте мережу в готелі чи кафе, переконайтеся, що точка доступу, до якої Ви входите, належить саме тому місцю, де ви зараз перебуваєте. Якщо Ви не впевнені у цьому, обмежте себе пошуком інформації та не використовуйте служби, які вимагають введення паролю. Слід обмежитись лише використанням веб-сайтів, які підтримують протокол HTTPS, або використанням VPN-тунелю.

12. Подбайте про паролі

Найкраще коли паролі не мають нічого спільного з Вашим особистим життям, місцем проживання, Вашим ім'ям та прізвищем, датою народження, іменами Ваших родичів чи домашніх тварин тощо, тобто інформацією, яку можна легко пов'язати з Вами, спостерігаючи за Вашою поведінкою в Інтернеті або поєднати з іншою інформацією про Вас.

Також не варто записувати їх на аркуші паперу або в зошит. Найкраще запам'ятати їх, а це важко,особливо коли Вам доводиться логуватися на багатьох веб-сайтах. Безкоштовні менеджери паролів можуть бути корисними в цьому питанні, оскільки вони дозволяють не тільки генерувати важкі для злому паролі,а й запам'ятовувати їх за Вас. Завдяки цьому легше частіше змінювати паролі, а ризик того, що хтось їх дізнається, зменшується.

Постійно змінюйте паролі до свого комп'ютера, електронної пошти, електронних банківських систем і навіть інтернет-магазинів, де у Вас є обліковий запис користувача. При цьому намагайтеся використовувати різні паролі.

13. Встановіть багаторівневу авторизацію

Багаторівнева авторизація є важливою, оскільки забезпечує додаткову безпеку під час входу. При отриманні доступу, крім введення пароля, користувачі повинні пройти додаткову перевірку особи, наприклад, ввівши код, отриманий на номер телефону.

14. Будьте обережні та пильні щодо оголошень про працевлаштування

Найпоширенішим прикладом можливої небезпеки втрати даних, є пошук роботи. На жаль, серед правдивих оголошень є й такі, які мають на меті отримати якомога більше докладної інформацію про Вас, тому варто дуже уважно аналізувати такий контент і бути особливо уважним, коли потенційний роботодавець хоче, щоб Ви, окрім базових та контактних даних про себе, також, наприклад, надали скани Ваших документів, що посвідчують особу, що не є необхідними в процесі найму. Рекомендовано використовувати офіційні сайти працевлаштування.

Будьте пильними

Зберігайте пильність, вона допоможе вберегти Ваші персональні дані перед потраплянням до рук неуповноважених лиць або осіб, серед яких можуть знаходитись особи (наприклад, злочинні групи, шахраї, викрадачі), які отриману в цей спосіб інформацію використовуватимуть незаконно.

- Не відповідайте на електронні листи від людей, яких Ви не знаєте, особливо коли вони просять Вас надати якусь інформацію про Вас або просять натиснути на посилання чи відкрити надіслане вкладення, пропонують змінити Ваш логін та пароль.
- Також будьте обережні, коли користуєтеся послугами електронного банкінгу та здійснюєте покупки через Інтернет.
- Переконайтеся, що Ви входите на веб-сайт інтернет-банкінгу з веб-сайту банку, який має сертифікат SSL (відображається в адресному рядку браузера).
- Перевіряйте магазини, в яких Ви хочете щось купити: чи існують вони взагалі, чи є у них відгуки, чи вони ідентифіковані, де вони розташовані, чи надається контакт з їхнім власником і чи цей контакт не обмежується лише електронним. Якщо у вас є сумніви щодо безпеки ваших даних, подумайте, чи дійсно Вам потрібно купувати щось у цього продавця.
- Перевіряйте правила та політику конфіденційності – уникайте продавців, які не надають таких документів або містять у них положення, які є занадто загальними, нечіткими чи неточними, сформульованими неправильно граматично чи лінгвістично, оскільки це може означати, що вони не підпадають під дію польського чи європейського законодавства.

Захист персональних даних дуже важливий. Захищаючи Ваші персональні дані належним чином, ми можемо обмежити ризик їх використання неуповноваженими особами.

КОРИСНІ КОНТАКТИ ОРГАНІЗАЦІЙ, ЯКІ ДОПОМАГАЮТЬ:

У зв’язку із складною ситуацією, спричинену нападом РФ на Україну, прибуло дуже багато біженців, шукаючи притулку і допомоги. Багато людей, організацій та установ допомагають біженцям вирішуючи найважливіші питання, такі як надання житла, харчування та медичного обслуговування.

У цьому контексті варто також мати на увазі, що особи, які перебувають на території Європейського Союзу, можуть скористатися правами, вміщеними у Загальному регламенті захисту персональних даних (RODO). У зв’язку з цим Організація Захисту Персональних Даних (UODO) створили спеціальну електронну адресу, за якою громадяни України, які перебувають на території Польщі, зможуть отримати всю необхідну інформацію, стосовно допомоги - forUkraine@uodo.gov.pl
Електронна скринька опрацьовуватиме звернення з 8:00 по 16:00.

- pomagamukrainie.gov.pl – це важлива адреса, якщо Ви шукаєте де переночувати, потребуєте гуманітарної допомоги, транспорту та підтримки в широкому розумінні;
- Рекламації, повернення товару та права споживача в Польщі — увійдіть на сайт Управління охорони конкуренції та споживачів (Urząd Ochrony Konkurencji i Konsumentów) — https://www.uakonsument.uokik.gov.pl/
- Корисні поради щодо користування послугами мобільних операторів можна знайти на сайті Управління електронної комунікації (Urząd Komunikacji Elektronicznej) — https://cik.uke.gov.pl/aktualnosci-cik/wszyscy-jestesmy-konsumentami,24.html
- Інформація про страхові компанії та банки — пошукова система — https://www.knf.gov.pl/en/CONSUMERS/Information_for_the_financial_market_consumers/Entities_search
- Дізнайтеся про свої права, пов'язані з користуванням фінансовими та страховими продуктами, а також як Вам може допомогти фінансовий омбудсмен (Rzecznik Finansowy) — https://rf.gov.pl/en/important-views/
- Інформація про подорожування залізницею. Дізнайтеся про свої права на сайті Управління залізничного транспорту (Urząd Transportu Kolejowego UTK) — www.utk.gov.pl/ukraina oraz https://www.utk.gov.pl/en/passenger-rights
- Якщо Ви плануєте виїхати з Польщі до іншої країни, дізнайтеся про основні права споживача під час подорожі до ЄС, Норвегії, Ісландії та Великобританії — https://konsument.gov.pl/aktualnosci/podroze-po-europie-twoje-prawa-konsumenta/
- Кожен, хто перебуває на території Європейського Союзу, може користуватися правами, закріпленими в RODO. Детальну інформацію про це, а також рекомендації щодо захисту персональних даних та конфіденційності, а також щодо безпечного користування Інтернетом можна знайти на сайті Управління захисту персональних даних (Urząd Ochrony Danych Osobowych) — https://uodo.gov.pl/p/forukraine

HOW TO EXERCISE THE RIGHTS GUARANTEED BY THE GDPR?

The General Data Protection Regulation – the act which is directly applicable in all Member States of the European Union, uniformly regulating citizens' rights and data controllers' obligations.

Personal data means information that allows your identity to be established. It is your name, surname, place of residence, telephone number or your e-mail address or location data.

Data processing means any activities that make use of personal data, such as collection, recording, structuring, storage, consultation, use or making available of data.
The GDPR grants natural persons many rights that allow them to have more control over their personal data.

The Personal Data Protection Office prepared 10 tips on how to exercise the rights guaranteed by the General Data Protection Regulation (GDPR).

You have the right to know what will happen with your data

You should know who, on what ground and why is processing your personal data. The company or institution that has obtained your data should inform you about it. It is also obliged to indicate your GDPR rights. You have the right, among others to: access your data, rectification, erasure, limitation of processing, portability, objection or the right to be informed about automated decision making, including profiling. In performing the information obligation, the controller must indicate how long it will store your data and provide the contact details of the Data Protection Officer (DPO), if the DPO has been designated.

You have the right to withdraw your consent at any time

If the informed and free consent expressed by you is the ground for the processing of your data, you have the right to withdraw it at any time and this cannot entail any negative consequences for you (e.g. increasing the service fee above its standard amount). Remember that withdrawal of consent should be as easy as giving it.

You should be informed in a way that is understandable to you

All information provided to you as regards the processing of your data should be formulated in a clear and plain language that is understandable to you. This also applies to information related to the use of Internet services or mobile applications. If you do not understand it or do not understand it enough, ask the controller for additional explanations. In Poland, the official language is Polish. All information must be in Polish, but it may be additionally translated into other languages.

You have the right to be forgotten, but not always

Although the GDPR has granted you the right to be forgotten (erasure of data), please note that it is not absolute. You can request the exercise of this right, e.g. in case where the data have become unnecessary for the intended purposes, the data have been processed unlawfully or you have withdrawn your consent and there is no other legal ground for their use.

Remember that in not every situation you have the right to be forgotten. This happens when a given entity (e.g. a school, a commune or a clinic) must use your

data to fulfil the legal obligation which is imposed on the entity.

You have the right to information about data breach

Data leakage, data loss or data disclosure to unauthorised persons – it happens. And this poses a serious threat to you, so do not be surprised that the controller informs you about it - this is the controller's obligation. Follow its instructions to minimise the threat. Sometimes, e.g. changing the password in the Internet system or putting a hold on the documents will allow you to protect your data and avoid, e.g. the identity theft and the related consequences, such as e.g. incurring loans on your behalf.

In case of doubts, contact the controller or Data Protection Officer who is designated by the controller. They should help you in this situation.

If you object to the processing of your data - marketing cannot be carried out

If your data is used for marketing purposes, i.e. to present you with offers of goods or services, you can object to this at any time. If you do this, your data may no longer be used for such purposes.

Protect children from unfair practices

If you are a parent or a legal guardian of a person under the age of 16, remember that when she or he uses the so-called information society services (provided electronically), e.g. social networks, applications or games, you decide on giving consent to the processing of his/her personal data. This is important, because children are often less aware of the risks and consequences of processing of their personal data. The GDPR indicates that special protection should be provided to them when their data is used for marketing purposes or for the creation of personal profiles. Pay attention to whether the messages addressed to them by the controller are formulated in a language that they can understand.

First request the controller to exercise your rights

If you think that someone is mishandling your data, contact him or her (or the appointed DPO) first and ask for explanations or fulfilment of your request, e.g. rectification of data, recording of objection, erasure of data

You can claim damages before a court

Remember! If the entity which is in possession of your data uses it contrary to the GDPR rules and you have suffered material or non-material damage as a result, you can claim damages from this entity by initiating the proceedings before a court. You have the right to do so regardless of the fact whether you intend to lodge a complaint with the President of Personal Data Protection Office or not.

HOW TO LODGE A COMPLAINT WITH THE PRESIDENT OF THE PERSONAL DATA PROTECTION OFFICE?

Anyone who believes that his or her personal data protection rights have not been respected may lodge a complaint against the controller with the President of the Personal Data Protection Office. Complaints may be submitted in written or electronic form.

The complaint shall be sent by electronic means through the Electronic Inbox of the President of the Office, after completing the FORM – i.e. "General letter to a public body" available on ePUAP2 portal.

Remember that each complaint must contain:
- your name and surname and address of residence;
- indication of the entity against which the complaint is lodged (name/name and surname, and address of the seat/residence);
- a detailed description of the violation;
- your request, i.e. indication of what action you expect from the Personal Data Protection Office (e.g. erasure of data, fulfilment of the information obligation, rectification of data, limitation of data processing, etc.);
- handwritten signature;

Remember to attach evidence confirming the controller's incorrect action (e.g. correspondence with the controller, contracts, certificates). This will make it easier for the Office's staff to assess the case.

Complaints which do not contain your name and address will not be further considered due to the impossibility of contacting you.

HOW TO PROTECT PERSONAL DATA?

Personal data are very valuable, as thanks to them you can gain access to many goods. However, they can also be used for marketing and sales purposes or, unfortunately, for criminal purposes. In order to better protect every person's personal data and to process them safely, special legislation which serves this purpose, that is the General Data Protection Regulation (GDPR), applies in the European Union.

The Personal Data Protection Office presents some of the most important tips on how to take care of your personal data

1. Be careful what and with whom you share about yourself online
It happens that you excessively share information about yourself, and in social media you share information about you, your assets, workplace, events from your everyday life, you share your location and upload photos. This makes the Internet a source of knowledge about your views, consumer behaviour and interests. These data allow, for example, marketing departments of various companies to adjust the offer addressed to you. But also fraudsters may use such information for criminal purposes. In particular, if your profile is fully public, you may be exposed to the risk of your data being used without your knowledge and consent, contrary to the purposes for which you provided the data.

2. Do not deposit identity documents
Pursuant to the law, retaining your identity card or passport without a legal basis is punishable. If you lose control over your identity card or passport, you are exposed to the possibility that the document may be used without your knowledge and will, which in turn poses the risk of identity theft.

3. Do not allow to make a photocopy
As a rule, you should not agree to the copying of your identity document. Only in certain situations, it is exceptionally permissible, when the law allows it. When the controller demands a copy of, for example, your ID card, ask him to indicate to you the legal basis that imposes an obligation on it to do so.
In other cases, such as renting equipment, this practice still exposes us to the same dangers. Therefore, do not agree to this.

4. Do not give data over the phone

Avoid providing data over the phone - especially if you are not the one initiating the call, but someone is calling you. Sharing data remotely is fraught with risk, with uncertainty as to whom the data is actually being provided.

Make sure to whom you in fact provide data during a phone call, and if necessary verify the contact, e.g. by calling back and checking whether the number and person actually represents the entity being referred to.

5. Be careful when sharing data through various forms

Be careful when filling out and signing various surveys, forms or contracts. Consider whether you really want to sign up for a shop loyalty card to get discounts or extra promotions. In such situations, you provide the shops with your name, surname, address of residence, date of birth, e-mail address, telephone number, and in return you receive promotions, discount vouchers, additional gifts when shopping.

Please, note that the controller must fulfil its information obligation towards you, i.e. provide you with the necessary information about itself, including its identity, contact details and the contact details of its Data Protection Officer (if it has appointed one), why, i.e. for what purpose and on what legal basis they process the data.

6. Avoid providing excessive data

Do not provide all data which allow for full identification, if it is not necessary in a given situation, i.e. excessive data. If you must use a given service, provide only the data necessary to perform that service - carefully consider providing data that is marked as optional.

7. I consent to...

Before you tick all the consents allowing for the processing of your personal data, make sure what they relate to. Pay attention to whether they are ticked by default on the consent form.

Also read carefully what the consent clauses refer to. In case of doubts, ask the controllers. They should inform you about the period for which the data will be processed and about your rights, including access to the data, rectification and erasure of data or expressing an objection to the processing, as well as whether your data will be transferred to someone else (other recipients).

Remember that you often give your consent to the use of data for marketing purposes not only of the controller, but also of its business partners. If you can, verify who they are, what companies these are. Consent for third-party marketing should be optional and you should be given a choice as to whether to give your consent or not.

The controller should ensure that the ability to withdraw consent is as easy as giving it and you should be informed of your right to withdraw consent before you give it.

8. Do not throw data in the rubbish until you have destroyed it

Any documents containing your data constitute another source of knowledge about you, especially if they contain a lot of different information allowing to draw conclusions about you. Therefore - before you throw documents in the rubbish bin - you should destroy them (e.g. invoices, bills, notes, stickers on correspondence packages or delivered goods) in a way that makes it impossible to recover personal data contained therein.

9. Permanently delete data from media

Huge amounts of data about you may be on your old hard drives, memory cards, memory sticks or other media. Note that more and more information about you is stored on computers, smartphones, cameras or tablets. Before you dispose of such devices or media, permanently delete the data on them. However, simply deleting them will not be enough as much of the data can be recovered. Therefore, before you

throw the media away or sell it, delete the data on it using the appropriate software. It is also a good idea to reset your device to factory settings, so that it does not remember logins and passwords to various services and applications you have used, especially those that you are still using.

10. Use mobile devices protection software

Use software that protects mobile devices, e.g. your smartphone or computer, against unwanted external activities such as malware. In addition to popular anti-virus software, software that protects against external interference called firewall may also be useful. Current updates are important. Malware, against which such tools protect us, is created every day. Therefore, without an up-to-date virus database and malicious applications database, an antivirus program will not fully fulfil its role.

11. Avoid public hotspots

Avoid "open" hotspots available to everyone in crowded places. If you use the network in a hotel or cafe, make sure that the access point to which you log in for sure belongs to the place where you are currently staying. If you are not sure, limit yourself to searching for information and do not use services that require a password. You should limit yourself to only using websites with HTTPS protocol or using a VPN tunnel.

12. Take care of passwords

It is a good idea for passwords to have nothing to do with your personal life, place of residence, your name and surname, date of birth, names of your relatives or pets, etc., i.e. information that can easily be associated with you by observing your online behaviour or linked to other information about you.

You should also not write passwords down on a piece of paper or in a notebook. It is best to remember them, which is a challenge when you have to log in to many services. Free password managers can be helpful in this regard, as they not only generate passwords which are difficult to break, but also remember them for us. This makes it easier to change your passwords more often, and reduces the risk of someone learning them.

Regularly change the passwords to your computer, e-mail, e-banking systems, but even online shops where you have a user account. Try to use different passwords.

13. Use multi-factor authentication

Multi-factor authentication is essential as it provides additional protection when logging in. When gaining access, in addition to entering a password, users must undergo additional identity verification, e.g. by entering a code received on a telephone number.

14. Be wary of advertisements

An example of a situation in which you are at risk of losing data is when you are looking for a job. Unfortunately, among the genuine advertisements there are also those aiming at obtaining as detailed information about you as possible. Therefore, it is worth to analyse such contents very carefully and be especially cautious when a potential employer wants you to provide not only basic information about you and contact details but also, for example, scans of your identity documents, which is not necessary in the recruitment process. It is worth using official job placement services.

Be vigilant

Be cautious, which may prevent your personal data from falling into the hands of unauthorised entities or persons, as they may include those (e.g. criminal groups, thieves, kidnappers) who will use the information obtained in this way illegally.

- Do not reply to emails from people whom you do not know, especially if they ask you for some information about yourself or encourage you to click on a link or open an attachment they have sent you, or suggest

you to change your user ID and password.
- Be careful also when using e-banking services and purchasing online.
- Make sure that you log in to your internet banking service from a bank website that has an SSL certificate (visible in the address bar of your browser).
- Verify shops, in which you want to buy something: do they exist at all, do they have opinions, are they identified entities, where are they based, is the contact with their owner given and is the contact limited only to electronic contact? If you have doubts about the security of your data, consider whether you absolutely need to buy from this seller.
- Verify terms and conditions as well as privacy policies - avoid sellers who do not present such documents or who present in them provisions that are too general, unclear or imprecise, grammatically or linguistically incorrect, as this may mean that they are entities not being subject to the Polish or European law.

The protection of personal data is very important. By adequately protecting your personal data, you can limit the risk of them being used by unauthorised persons.

USEFUL CONTACTS TO INSTITUTIONS PROVIDING HELP:

Due to the difficult situation caused by the attack of the Russian Federation on Ukraine, many refugees came to Poland seeking shelter and help. Many individuals, organizations and institutions are involved in providing assistance, taking care of the most important issues, such as providing accommodation, food or medical care.

It is also worth bearing in mind in this context that people who are in the territory of the European Union can benefit from the rights given to them by the GDPR. Therefore, the Personal Data Protection Office (UODO) launches a special e-mail address where Ukrainian citizens staying in Poland will be able to obtain any information in this respect - forUkraine@uodo.gov.pl .
This e-mail is serviced on weekdays from 8 a.m. to 4 p.m.

- An important website if you are looking for accommodation, humanitarian aid, transport and broadly understood assistance – pomagamukrainie.gov.pl.
- For information on complaints, product returns, regulations and rights applicable in Poland in contacts between consumers and traders (sellers, service providers) go to the website of the Office of Competition and Consumer Protection – https://www.uakonsument.uokik.gov.pl/
- Useful tips on how to use the services of telecommunications operators can be found on the website of the Office of Electronic Communications - https://cik.uke.gov.pl/aktualnosci-cik/wszyscy-jestesmy-konsumentami,24.html
- Information on insurers and banks - entity search engine - https://www.knf.gov.pl/en/CONSUMERS/Information_for_the_financial_market_consumers/Entities_search
- Learn about your rights when using financial and insurance products and how the Financial Ombudsman can help you - https://rf.gov.pl/en/important-views/
- Information on rail travel. Learn about your rights and options on the website of the Office of Rail Transport (UTK) - www.utk.gov.pl/ukraina and https://www.utk.gov.pl/en/passenger-rights

- If you are planning to travel from Poland to another country, read the basic information on consumer rights when travelling in the EU, Norway, Iceland and the UK - https://konsument.gov.pl/aktualnosci/podroze-po-europie-twoje-prawa-konsumenta/

- Persons residing in the European Union can exercise their rights under the GDPR regulation. For more information on this topic and tips on how to protect your personal data and privacy and how to navigate the Internet safely, go to the website of the Personal Data Protection Office - https://uodo.gov.pl/p/forukraine

URZĄD OCHRONY DANYCH OSOBOWYCH