Ochrona danych osobowych- część II

Wykład 1 rok informatyki algorytmicznej

Mirosław Kutyłowski 2021

Katedra Podstaw Informatyki

STAN OBECNY:

- **General Data Protection Regulation (GDPR, po polsku RODO) – rozporządzenie na poziomie UE, bezpośrednio stosowane w krajach UE**
- **nie wymaga implementowania przez Sejm, nie może być ani poprawione ani zepsute przez lokalne władze**

- **GDPR uchwalone w 2016, okres dostosowawczy do 2018 *(praktycznie do 2018 niewielka aktywność)***
- ***od 2018 teoretycznie wdrożone, w praktyce rażące naruszenia ignorowane przez organy nadzoru***

- **Kontrowersje: techniczna implementowalność, hamowanie analizy danych**

CELE:

- **jednolite wymagania na Wspólnym Rynku *(redukcja kosztów i ryzyka działalności!)***
- **ochrona danych osobowych również po ujawnieniu, właścicielem pozostaje osoba, której dane dotyczą**
- **bezpieczeństwo na drodze technicznej i organizacyjnej a nie wyłącznie za pomocą sankcji za naruszenia**
- **rozliczalność działań**

Zakres materialny RODO

1. **This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.**

Wszystko w systemach IT jest przetwarzaniem „by automated means". Chodzi również o dane, które znajdą się w „filing systems", czyli systematycznych zbiorach danych – nawet papierowych i/lub tworzonych ręcznie.

Zakres materialny – wyjątki:

2. **This Regulation does not apply to the processing of personal data:**

(a) in the course of an activity which falls outside the scope of Union law;

(b) ...

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Czyli użytek czysto osobisty nie jest w zakresie GDPR, ale działalność religijna, polityczna, związkowa, … jest podporządkowana RODO!

Zakres terytorialny:

1. **This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.**

Przetwarzanie danych osobowych przez podmioty europejskie, nawet gdy fizycznie przetwarzanie wykonują poza UE (np. na Islandii)

Zakres terytorialny:

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services , irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

Chodzi m.in. o Google, Microsoft, Facebook, Twitter, WeChat, Whatsapp, Ebay, Aliexpress, Netflix,...

Nie tylko sprzedaż i usługi ale i o profilowanie kilentów

Dane osobowe:

Bardzo szeroki zakres pojęcia (dawniej tylko dane takie jak PESEL, miejsce zamieszkania, itp.):

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’);

an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Dane osobowe:

Problemy:

- **Pewne sytuacje są oczywiste: np. gdy jest podany PESEL wtedy dane są osobowe**
- **Inne mogą być nieoczywiste:**

„student o numerze indeksu <tu konkret> najlepiej napisał kolokwium”

- **Kto ma powiązać dane z osobą? Możliwa sytuacja:**

a) osoba A umie powiązać dane D z osobą X, zaś

b) dla osoby B nie jest możliwe powiązanie D z żadną osobą.

np.: D jest kryptogramem, ale szyfr jest na tyle słaby że agencja wywiadu A umie złamać zabezpieczenia

Przetwarzanie danych osobowych:

źródło etymologiczne: „cyfrowe przetwarzanie informacji”, „digitale Datenverarbeitung” – w istocie nic nie „przetwarzamy” tylko „obsługujemy”

‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

.. czyli każda operacja, łącznie z usuwaniem, inaczej niż w potocznym rozumieniu

Profilowanie

‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person , in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Zasadniczy element wielu serwisów i podstawy ich ekonomicznego funkcjonowania – serwisy „za darmo” ale płacimy poprzez ekspozycję na sprofilowaną reklamę.

Firmy oferujące darmowe serwisy dostają w zamian dane np.. o istniejących trendach. Te dane są cenne (np. dla ochrony zdrowia). Czy wolno z nich korzystać?

Controller, Processor:

„controller” – jednostka, która kontroluje proces przetwarzania danych osobowych (ale niekoniecznie to sama robi)

„processor” – jednostka, która w sensie technicznym wykonuje czynności przetwarzania danych osobowych

W wielu krajach poza UE nie ma takiego rozróżnienia.

Czasami „joint controllers”.

Paradygmaty:

- **Kilka zasad które zasadniczo zmienia podejście do ochrony danych w stosunku do przeszłości**

- **Ukierunkowane na ochronie prywatności jako fundamentalnego prawa ...**

- **… ale w istocie chodzi o bezpieczeństwo**

Ps: zasady te są wciąż powszechnie łamane

lawfulness, fairness and transparency

Personal data shall be:

processed lawfully, fairly and in a transparent manner in relation to the data subject

Konsekwencje:

1) podstawa prawna lub zgoda na przetwarzanie jest niezbędna.
– bez tego przetwarzanie jest przestępstwem.

2) dane muszą być prawdziwe, obowiązek korygowania błędów
– teoretycznie można domagać się skorygowania fałszywych danych

3) „data subject” ma prawo wiedzieć jakie jego dane i jak są przetwarzane

Purpose limitation

collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

Zmiana celu przetwarzania niedozwolona. Cele muszą być explicite znane. Wyjątek: cele naukowe, historyczne, interes publiczny (nie naruszajacy wolności i interesów jednostki)

Data minimisation:

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ;

Konsekwencje:

- ***tradycja: gromadzić jak najwięcej danych***
- ***… ale więcej danych to większe zagrożenie w przypadku włamania***

- **Data minimisation ogranicza możliwości przetwarzania danych pod pretekstem**

Accuracy:

accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

Konsekwencje:

- ***prawo do skorygowania danych – na żądanie „data subject”***
- ***źródło problemów: wiele kopii, nie wszystkie wiadomo gdzie są, proces usuwania śladów cyfrowych może długo trwać***

Storage limitation:

kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes … subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject;

Konsekwencje:

- *ścisła reglamentacja przechowywania danych*
- *wyjątki: prawa i wolność jednostki muszą być respektowane*

Integrity and confidentiality:

processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures .

Konsekwencje:

- ***gwarancje bezpieczeństwa muszą wynikać z samego sposobu przetwarzania (a nie oparte na deklaracjach czy odpowiedzialności stron)***
- ***Srodki techniczne i organizacyjne wskazane explicite***

Accountability:

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1

Konsekwencje:

– obowiązek implementacji zasad i odpowiedzialność za to po stronie przetwarzającego dane (privacy-by-design)

- obowiązek wykazania zgodności z zasadami (provable privacy)

Realia:

– w większości przypadków to jeszcze science fiction a nie stan techniki

Consent:

- **gdy nie ma obowiązku prawnego przetwarzania danych (np. dane osobowe przetwarzane w związku z ustawą o podatku VAT), to zwykle wymagana jest zgoda osoby, której dane dotyczą**
- **zasada przestrzegana przez firmy: nawet do przesady (występowanie o zgodę nawet gdy nie jest to potrzebne)**
- **poza tym zasada powszechnie łamana: np. zjawisko paparazzi, ataki na osoby o innych poglądach, …**

Consent:

- zgoda musi być explicite, nie może być dorozumiana z innej czynności

Dopuszczalność przetwarzania danych osobowych:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

Dopuszczalność przetwarzania danych osobowych:

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

np. kwestie epidemiologiczne, dostęp do danych medycznych nieprzytomnego pacjenta

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

ale organy publiczne działają jedynie w granicach prawa: musi istnieć explicite obowiązek ustawowy

Dopuszczalność przetwarzania danych osobowych:

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party , except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Nie można zażądać zaprzestania przetwarzania danych osobowych wierzycielowi ...

- **Consent:**

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

Trudno wykazać, że użytkownik kliknął i co kliknął.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

Nie ma możliwości rozciągnięcia zgody na inne sprawy.

Consent:

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Usunięcie zgody implikuje konieczność zaprzestania przetwarzania.

Dzieci:

- **szczególne warunki związane z przetwarzaniem danych osobowych dzieci – ochrona dzieci**
- **wymagana zgoda rodzica/opiekuna prawnego dla dzieci w wieku poniżej 16 lat**

ale brak jest powszechnego wsparcia technicznego do weryfikacji wieku (poza Belgią, …)

Dane wrażliwe:

- **Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation**

shall be prohibited.

Są określone wyjątki (np. związki zawodowe mogą na swoje potrzeby przetwarzać dane swoich członków).

Dane wrażliwe – dane medyczne:

processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

wykorzystanie danych medycznych poza systemem ochrony zdrowia/ubezpieczeń społecznych/medycyny pracy dla innych celów jest zabronione

Dane medyczne – kontrowersje:

- *stan zdrowia osoby posiadającej dostęp do broni jądrowej – czy powinien być tajemnicą?*

- *przypadek samobójstwa pilota Germanwings 9525 we Francji, 150 ofiar pilota chorego psychicznie,*

tajemnica lekarska psychiatry pilota

Transparent information, communication and modalities for the exercise of the rights of the data subject:

- *Szereg wymagań odnoszących się do zrozumiałości i adekwatności informacji.*
- *Ciężar dowodu często po stronie przetwarzającego dane osobowe.*
- *Data subject może żądać a nie tylko wnioskować dostęp do informacji na swój temat.*
- *Termin 1 miesiąca na odpowiedź.*

> implementacja procedur, istotne koszty, niezbędne umiejętności w zakresie edycji informacji

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

Right-to-be-forgotten

- „prawo do bycia zapomnianym”: prawo do żądania usunięcia danych osobowych (np. zdjęć o czysto prywatnym,
- regulacja powstała po sporze Google-Hiszpania i sankcjach finansowych ze strony Francji
- kontrowersje: praktyka lekarska/stomatologiczna prowadzona pod własnym nazwiskiem, zła jakość usług medycznych – żądania usunięcia komentarzy byłych pacjentów opisujących fakty z przebiegu leczenia
- problem: bezwarunkowe prawo do bycia zapomnianym może naruszać wolności i interesy innej osoby

Dokładne brzemienie uprawnień do bycia zapomnianym:

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based ..., and where there is no other legal ground for the processing;

(c) the data subject objects to the processing … and there are no overriding legitimate grounds for the processing, …

Dokładne brzemienie uprawnień do bycia zapomnianym:

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Prawo do bycia zapomnianym – wyjątki:

3. **Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:**

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

Prawo do bycia zapomnianym – wyjątki:

3. **Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:**

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Automated individual decision-making, including profiling

1. **The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.**

- ***problem dla systemów tzw. sztucznej inteligencji***
- ***konieczność wdrożenia manualnych procedur***

Obowiązki podmiotu przetwarzającego dane osobowe

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

Data protection by design and by default

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Data protection by design and by default

- *wymagania adekwatne do potrzeb*
- *wystarczy postępować zgodnie z bieżącym stanem sztuki*
- *wspomniana pseudonimizacja może być niewystarczająca (pseudonimizacja – zastąpienie identyfikatorów pseudonimami – ale operacja odwracalna)*

(więcej o pseudonimizacji: na zajęciach na wyższych latach)

Incydenty bezpieczeństwa

- **wcześniejsza praktyka: ukrywać, by nie naruszać swojej reputacji na rynku**
- **teraz: obowiązek informowania organów nadzoru, a również w uzasadnionych przypadkach również osoby, których dane zaatakowano**

- **mogą wystąpić problemy z kontaktem z osobami fizycznymi: przechowywanie danych kontaktowych to dodatkowe zagrożenie**

Data protection impact assessment

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

Należy samemu zbadać czy przetwarzanie danych nie spowoduje negatywnych konsekwencji

Data protection officer

Obowiązkowe stanowisko:

- **w instytucjach publicznych (oprócz sądów)**
- **gdy przetwarzanie „require regular and systematic monitoring of data subjects on a large scale”**

Rola:

- **kontrolna, nie zajmuje się bieżącym administrowaniem systemem**
- **rola analogiczna do oficera politycznego w jednostkach Armii Czerwonej (bieżąca kontrola działania jednostki a nie dowodzenie)**

Data protection officer

Kwalifikacje:

The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in...

Potrzebni eksperci w zakresie prawa i informatyki,

w praktyce informatycy mało zainteresowani i obowiązki przejmowane przez osoby bez wiedzy inżynierskiej.

Problemy transgraniczne

Ograniczenia w transferze danych osobowych poza obszar obowiązywania RODO/obszarów uznanych za równoważne (niektóre kraje) czy podmioty stosujące Privacy Shield (USA, Szwajcaria)

Wymagane zgody organów nadzorujących

Organy nadzorujące

- **W każdym kraju odrębne organy nadzorujące (niekiedy więcej niż jeden – Niemcy ze względu na federacyjny ustrój państwa), w Polsce Urząd Ochrony Danych Osobowych**
- **European Data Protection Board: na poziomie europejskim jako organ koordynacyjny**
- **European Data Protection Supervisor – dla instytucji unijnych**

w praktyce niewiele pomocy ze strony organów nadzorujących dla przedsiębiorców, instytucji, …

stosunkowo dużo praktycznych informacji ze strony niemieckich organów i EDPS

Organy nadzorujące – sankcje

W odróżnieniu od poprzednich regulacji wysokość kar administracyjnych mogą być drakońskie:

Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: ...

w przypadku innych nieprawidłowości górne granice wynoszą 20 000 000 EUR lub 4 % obrotu

w przypadku mniejszych podmiotów maksymalna wysokość kar jest większa niż ich wartość.