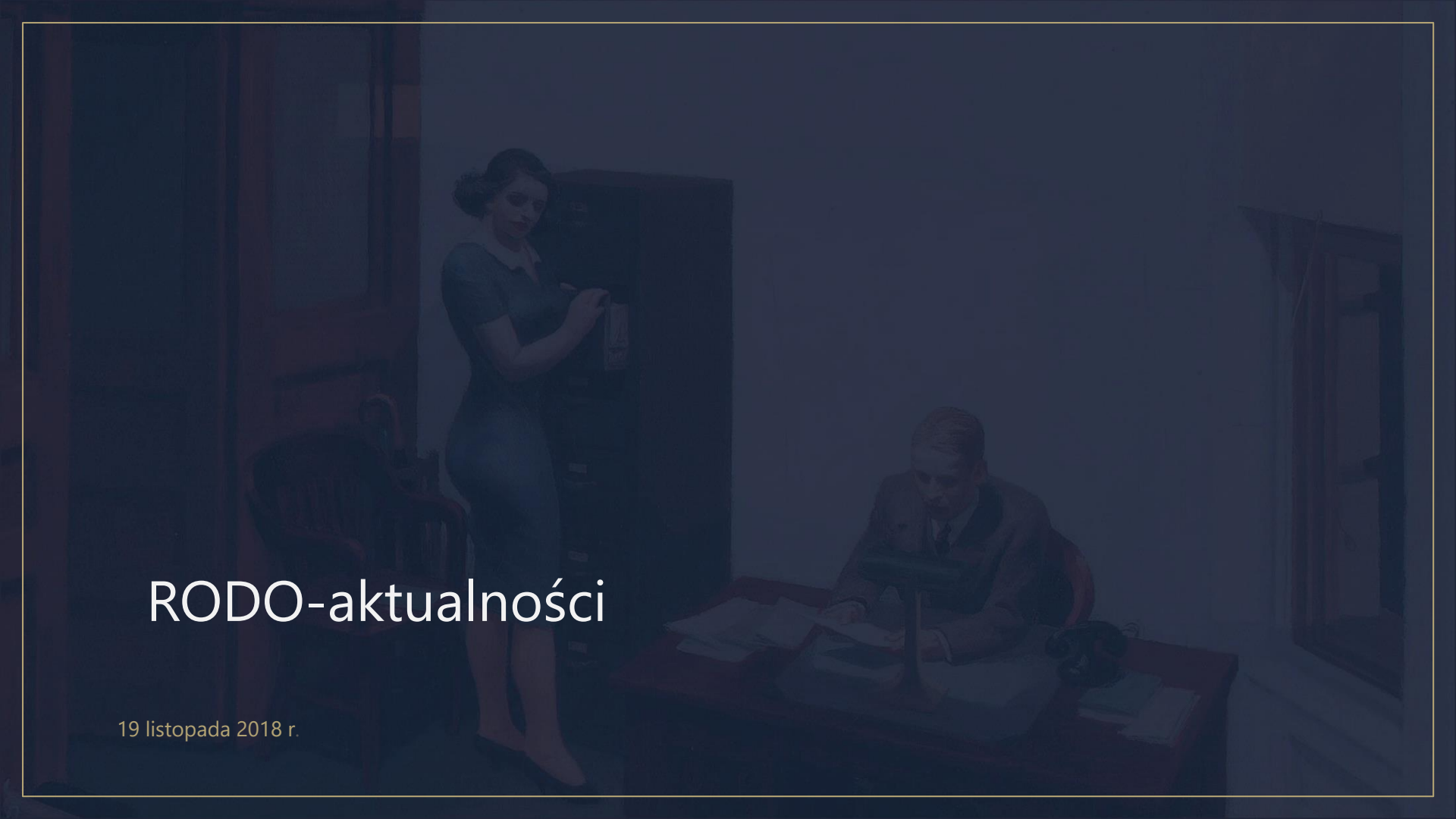
LEX ARTIST



RODO-aktualności

19 listopada 2018 r.

UWAGA!

Tezy przedstawione w artykułach, zamieszczonych w niniejszym materiale i niebędących wytycznymi organu nadzorczego albo orzeczeniem sądowym/organu administracji publicznej, stanowią wyłącznie opinię ich autorów i nie są oficjalnym stanowiskiem Lex Artist Sp. z o.o.

LEX ARTIST

Spis treści

1 Zaciska się pętla wokół Facebooka

2 Firmy amerykańskie na celowniku fundacji

3 Krytyka polskiego wykazu operacji wymagających oceny skutków

4 Prawo spółdzielcze do poprawki?

5 Branża medyczna melduje: kodeks gotowy!

6 Wielka Brytania będzie państwem trzecim?

7 Orange ukarany za spam SMS

8 RODO wykorzystywane przeciwko dziennikarzom

9 WordPress ofiarą ataku

10 Microsoft Office prześwietlony przez holenderski rząd

LEX ARTIST

Spis treści

11 Irish DPIA

12 Pracodawco, potrzebujesz dwóch zgód na przetwarzanie wizerunku pracownika

13 Jak ugryźć rekrutacje ukryte?

14 Wytyczne dla archiwów

15 DPIA po portugalsku

16 Skarga na Twittera

17 RODO, a listy do M.

18 Takie będzie RODO, jak młodzieży wychowanie

19 Nie ma RODO dla złodziei

LEX ARTIST

Zaciska się pętla wokół Facebooka

1

- Brytyjski organ nadzoru (ICO) złożył skargę na Facebooka do irlandzkiej Komisji Ochrony Danych (DPC).
- ICO w raporcie (113 stron) wskazała, że odkryła na Facebooku „niepokojący brak poszanowania prywatności wyborców" i targetowanie osób fizycznych poprzez mechanizmy Big Data.

Źródło: https://www.compliancejunction.com/facebook-facing-gdpr-investigation-over-audience-targeting-methods/?platform=hootsuite

Firmy amerykańskie na celowniku fundacji

- Organizacja Privacy International z Wielkiej Brytanii złożyła szereg skarg przeciwko firmom z siedzibą w USA (m. in. Oracle, Acxiom czy Tapad).
- Przedsiębiorstwom zarzuca się gromadzenie (bez wiedzy i zgody użytkowników) dużej ilości ich danych osobowych, a następnie budowaniu w oparciu o nie skomplikowanych profili osób fizycznych.

Źródło: https://www.compliancejunction.com/uk-based-privacy-protection-group-focuses-on-gdpr-breaches-by-us-firms/?platform=hootsuite

LEX ARTIST

Krytyka polskiego wykazu operacji wymagających oceny skutków

- Europejska Rada Ochrony Danych otrzymała od UODO zmodyfikowany wykaz operacji wymagających przeprowadzenia DPIA – modyfikacje nastąpiły na skutek krytycznych uwag EROD z początku października 2018 r.
- Polskiemu wykazowi zarzucono: błędne zastosowanie zamkniętego katalogu operacji, oparcie obowiązku przeprowadzenia DPIA tylko na jednym (z 9) kryteriów wskazanych przez Grupę Roboczą art. 29 (powinny być spełnione dwa), brak wskazania czynności przetwarzania dotyczących monitorowania lokalizacji oraz brak przejrzystości wykazu.

Źródło: https://www.prawo.pl/biznes/ocena-ryzyka-przetwrzania-danych-wykaz-czynnosci-uodo-ma-wady,325350.html

Prawo spółdzielcze do poprawki?

- Z potencjalnym naruszeniem zasady minimalizacji danych oraz ograniczenia celu mamy do czynienia w art. 30 prawa spółdzielczego.
- Zgodnie z tym przepisem, prawo do przeglądania rejestru członków spółdzielni mają nie tylko członkowie, ale także ich małżonkowie oraz wierzyciele.
- Praktyką jest umożliwienie np. wierzycielowi wglądu do pełnego rejestru, wynika ona z literalnej interpretacji przepisu. Wierzyciel ma zatem możliwość wgląd do danych osobowych pozostałych spółdzielców, często jest to kilkaset osób.
- Konieczna może być interpretacja organu nadzoru (PUODO).

Źródło: https://prawo.gazetaprawna.pl/artykuly/1345630,spoldzielnie-naruszaja-rodo-udostepniajac-wierzycielowi-dane-jednego-dluznika-pokazuja-cale-rejestry.html

Branża medyczna melduje: kodeksy gotowe!

- Dwa projekty kodeksów postępowania dla branży medycznej zostały przekazane UODO do zatwierdzenia.
- Proponowaną granicą „dużej skali" wg projektu kodeksu jest liczba 600 unikalnych pacjentów.
- Prezydium Naczelnej Rady Lekarskiej wnioskuje jednak o zwiększenie tego limitu – kodeks wg NRL powinien zawierać stwierdzenie, iż incydentalne, występujące w jednym kwartale i nie wynikające z przyczyn strukturalnych przekroczenie limitu 600 pacjentów nie powoduje od razu uznania przetwarzania za dużą skalę.
- Wniosek o zatwierdzenie oraz projekt kodeksu można znaleźć tutaj.
- W przygotowaniu są kolejne dwa kodeksy dla branży medycznej, które dotyczą: biobankowania oraz działalności uczelni medycznych i szpitali klinicznych.

Źródła: http://www.infodent24.pl/lexdentpost/rodo-i-przetwarzanie-danych-na-duza-skale,110995.html

http://www.politykazdrowotna.com/38732,rodo-zdrowotny-kodeks-branzowy-trafil-juz-do-zatwierdzenia-przez-urzad

https://www.prawo.pl/zdrowie/kodeks-branzowy-dla-ochrony-zdrowia-dwa-projekty-zlozone-do-uodo,329952.html

Wielka Brytania będzie państwem trzecim?

- Tak, jeżeli dojdzie do tzw. twardego brexitu (wyjścia UK z UE bez porozumienia z Komisją Europejską).
- Częścią porozumienia dot. wyjścia UK z UE jest regulacja, że w okresie 2 lat po brexicie nadal będą obowiązywać dotychczasowe zasady.
- Wstępny projekt porozumienia zakłada, że między 29 marca 2019 r. a 31 grudnia 2020 r. (okres przejściowy) będą obowiązywały reguły dotychczasowe, natomiast UK będzie starać się o to, by Komisja Europejska wydała później (od 1 stycznia 2021 r.) decyzję w sprawie odpowiedniego poziomu ochrony.

Źródła: https://prawo.gazetaprawna.pl/artykuly/1345904,rodo-a-brexit-bedzie-wiecej-obowiazkow.html

https://www.twobirds.com/en/news/articles/2018/global/data-protection-and-the-draft-brexit-agreement-first-impressions#__prclt=bgNt5Y85

Orange ukarany za spam SMS

- Urząd Komunikacji Elektronicznej nałożył na Orange Polska S.A. karę 9,1 mln zł za wysyłkę niezamawianego spamu SMS (naruszenie art. 172 ust. 1 Prawa telekomunikacyjnego).
- Na decyzję regulatora miało wpływ to, że operator nie był w stanie wykazać (nie zapewnił rozliczalności) zgody na użycie automatycznych systemów wywołujących dla celów marketingu bezpośredniego.

Źródło: https://czasopismo.legeartis.org/2018/11/orange-kara-esemesowy-spam.html

RODO wykorzystywane przeciwko dziennikarzom

- Rumuński organ ochrony danych (ANSPDCP) zażądał dostępu do wszystkich systemów informatycznych od dziennikarzy badających sprawę defraudacji środków unijnych.
- Organ nadzoru przytacza RODO jako postawę do ujawnienia wszystkich informacji objętych tajemnicą dziennikarską.
- Dziennikarze uważają, że to kolejna próba zamknięcia im ust przez rumuńskie władze (wcześniej nasyłano na nich kontrolę podatkową).

Źródło: https://www.occrp.org/en/27-ccwatch/cc-watch-briefs/8878-romania-orders-journalists-investigating-corruption-to-give-up-sources

WordPress ofiarą ataku

- Przedmiotem ataku była wtyczka WP GDPR Compliance, która umożliwiała m. in. zażądania od administratora kopii danych.
- Hakerzy wykorzystali lukę zabezpieczeń wtyczki na dwa sposoby, co umożliwiło im na instalowanie na serwerach lokalnych złośliwego oprogramowania.
- Wordfence (firma bezpieczeństwa WordPress) naprawiła już lukę.

Źródło: https://nakedsecurity.sophos.com/2018/11/13/wordpress-gdpr-compliance-plugin-hacked/

Microsoft Office prześwietlony przez holenderski rząd

- Usługi Microsoft, które są wdrażane w ramach holenderskiej administracji publicznej, zostały poddane ocenie skutków dla ochrony danych.
- Wyniki są niepokojące. Według raportu Microsoft gromadzi i przechowuje dane osobowe dotyczące zachowania poszczególnych pracowników na dużą skalę i bez żadnej publicznej dokumentacji.
- Autorzy raportu stawiają również tezę, że Microsoft występuje w roli odrębnego administratora danych (ustala bowiem samodzielnie aż 7 celów przetwarzania danych, na co nie ma wpływu np. pracodawca).

Źródła: *https://www.privacycompany.eu/en/impact-assessment-shows-privacy-risks-microsoft-office-proplus-enterprise/*

https://mspoweruser.com/dutch-regulator-rule-microsofts-telemetry-fall-foul-of-gdpr-regulations/

Irish DPIA

- DPC (irlandzki organ ochrony danych osobowych) opublikował 15 listopada wykaz operacji przetwarzania danych, dla których wymagana jest DPIA.
- Katalog dotyczy głównie: profilowania (w szczególności osób szczególnie chronionych, w tym dzieci), przetwarzania danych biometrycznych, przetwarzania danych genetycznych, pozyskiwania danych osobowych w sposób pośredni, gdy wymogi w zakresie przejrzystości nie są spełnione, istnieje również wiele odwołań do „dużej skali".

Źródło: https://dataprotection.ie/documents/Data-Protection-Impact-Assessment.pdf

Pracodawco, potrzebujesz dwóch zgód na przetwarzanie wizerunku pracownika

- Autor artykułu, na przykładzie praktycznym, stawia tezę, że aby legalnie przetwarzać wizerunek pracowników np. w folderze reklamowym firmy kierowanym do klientów, należy posiadać dwie zgody: na rozpowszechnianie wizerunku (Prawo autorskie) oraz na przetwarzanie danych osobowych (RODO).
- Zgoda, wg autora, powinna być stosowana dlatego, że Kodeks pracy wśród kategorii danych, które pracodawca może (niedługo: będzie zobowiązany) przetwarzać nie ma wizerunku, a pozostałe kategorie danych można przetwarzać za zgodą pracownika.
- Zaznaczone jest także, że nie można pozbawić pracownika prawa do wycofania zgody.

Źródło: https://serwisy.gazetaprawna.pl/praca-i-kariera/artykuly/1348788,zdjecie-pracownika-w-folderze-reklamowym-obowiazki-pracodawcy.html,komentarze-najnowsze,1

Jak ugryźć rekrutacje ukryte?

- Artykuł wskazuje, w jaki sposób można prowadzić rekrutacje ukryte w zgodzie z RODO.
- Po pierwsze, potencjalny pracodawca może skorzystać z agencji zatrudnienia, która spełnia pierwotny obowiązek informacyjny, a następnie pozyskuje zgodę na udostępnienie danych osobowych kandydata do firmy poszukującej pracownika.
- Po drugie, w razie korzystania przez potencjalnych pracodawców z serwisów internetowych jak np. pracuj.pl (które to występują w roli procesorów), autorzy proponują probiznesową interpretację art. 13 ust. 1 RODO, a konkretniej sformułowania „podczas pozyskiwania danych osobowych".
- Wg autorów, potencjalny pracodawca mógłby spełnić obowiązek informacyjny po otrzymaniu zgłoszenia w formie e-maila zwrotnego. RODO bowiem nie stanowi wprost, że obowiązek informacyjny ma być spełniony wyłącznie w momencie poprzedzającym faktyczne pozyskanie danych.

Źródło: https://serwisy.gazetaprawna.pl/praca-i-kariera/artykuly/1348794,ukryta-rekrutacja-a-rodo.html

Wytyczne dla archiwów

- Europejska Grupa ds. Archiwów przygotowała wytyczne dot. wdrożenia RODO przez służby archiwalne – zarówno publiczne, jak i prywatne.
- Wytyczne (póki co w wersji angielskiej) można pobrać w tym miejscu.

Źródło: https://ec.europa.eu/info/sites/info/files/eag_draft_guidelines_1_11_0.pdf

DPIA po portugalsku

- CNPD (portugalski organ ochrony danych) opublikował listę operacji przetwarzania danych, które wymagają DPIA.
- Są to głównie operacje, które polegają na: profilowaniu, śledzeniu lokalizacji, przetwarzaniu danych biometrycznych, łączeniu wielu dużych zbiorów danych oraz w których nie jest możliwe zapewnienie prawa do informacji.

Źródło: https://eurocloud.org/news/article/list-of-personal-data-processing-activities-that-must-be-subject-to-a-data-protection-impact-assessm/

Skarga na Twittera

- Jeden z badaczy z University College London złożył do Twittera (siedziba w Irlandii dla UE) żądanie dostępu do swoich danych osobowych, a konkretniej informacji o tym, w jaki sposób Twitter go śledzi za pomocą skróconych linków.
- Twitter odmówił spełnienia żądania ze względu na „nieproporcjonalny wysiłek".
- Naukowiec złożył skargę do DPC (irlandzkiego organu), która aktualnie bada sprawę i stwierdzi, czy odmowa spełnienia żądania nie była naruszeniem RODO. DPC rozważa również zaangażowanie Europejskiej Rady Ochrony Danych w sprawę.

Źródło: https://www.itpro.co.uk/general-data-protection-regulation-gdpr/32141/twitter-faces-gdpr-probe-for-refusing-to-comply-with

RODO, a listy do M.

- RODO-absurdów ciąg dalszy. Władze powiatu w Niemczech (Frankonia Środkowa) odwołały w tym roku jedną z cyklicznych imprez w mieście Roth, jaką jest wieszanie listów do Św. Mikołaja przez dzieci ze szkół na choince miejskiej.
- Organizatorzy argumentują, że notatki dzieci były dostępne dla wszystkich, a znajdują się tam **dane wrażliwe** jak imię, wiek czy adres.
- Miejski inspektor ochrony danych zalecił, aby dzieci wypełniały kilka stron formatu A4 np. zgody, oświadczenie o zapoznaniu się z klauzulą informacyjną, jednak dzieci nie mogą tego robić.

Źródło: https://wize.life/themen/wissen/88333/wunschzettel-aktion-fuer-kinder-zu-weihnachten-gestoppt---dsgvo-sorgt-fuer-naechstes-chaos

Takie będzie RODO, jak młodzieży wychowanie

Życie Panie Życie .... odrabiam lekcje z moim IV-klasistą, zadanie "Opisz swojego kolegę z klasy". Zaczynamy, Imię ..... Nazwisko .....i tu pada z ust mojego syna ..... TATUŚ ALE PRZECIEŻ RODO 🤣

Coś drgnęło w edukacji .... oby poszło w dobra stronę.

Źródło: https://twitter.com/lol_rodo/status/1062619369899884544

Nie ma RODO dla złodziei

- W jednym ze sklepów Żabka w Toruniu na witrynie zawieszono fotografie osób, które zostały przyłapane na kradzieży.
- Właściciele sklepu: osoby kradnące na terenie obiektu wyrażają zgodę na publikację swojego wizerunku na portalach społecznościowych i witrynie sklepu. Złodziej, które nie wyraża na to zgody, proszony jest o opuszczenie sklepu.

Źródło: https://innpoland.pl/148029,zabka-w-toruniu-wywiesza-zdjecia-osob-przylapanych-na-kradziezy

Maciej Zychowicz

specjalista ds. ochrony danych osobowych

Niniejszy dokument bez zezwolenia nie może być w żaden sposób wykorzystywany,
w szczególności rozpowszechniany i kopiowany.

© Lex Artist Sp. z o.o., 2018