HEVELIANUM
80-802 Gdańsk, ul. Gradowa 6
REGON 190572660, NIP 583-000-93-15
tel. 58 300-08-42, fax 58 742-15-12

Zarządzenie nr ...61.../2019
Dyrektora Hevelianum
z dnia ...01... sierpnia 2019 roku

w sprawie wprowadzenia Instrukcji postępowania w przypadku wybranych zdarzeń przy przetwarzaniu danych osobowych w Hevelianum

Na podstawie art. 33 i 34 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) Dz. Urz. UE L z 2016 r. nr 119/1.

zarządzam, co następuje:

§1.

Wprowadzam „Instrukcję postępowania w przypadku wybranych zdarzeń przy przetwarzaniu danych osobowych w Hevelianum", która stanowi załącznik do niniejszego Zarządzenia.

§2.

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
HEVELIANUM
Paweł Golak

Joanna Januszewicz - Sierant
RADCA PRAWNY
Nr GD. 1182

Załącznik nr 1
do zarządzenia nr 61./2019
Dyrektora Hevelianum
z dnia 01 sierpnia 2019 r.

INSTRUKCJA postępowania w przypadku wybranych zdarzeń przy przetwarzaniu danych osobowych w Hevelianum

I. Procedowanie żądania osób, których dane osobowe są przetwarzane (właściciela danych).

1. Właściciele danych, których dane osobowe przetwarzane są przez Hevelianum mają prawo do:

1) dostępu do swoich danych,
2) otrzymania kopii danych osobowych ich dotyczących,
3) sprostowania swoich danych, jeśli są błędne lub nieaktualne,
4) żądania usunięcia danych, w sytuacji, gdy przetwarzamy dane na podstawie wcześniej udzielonej zgody,
5) ograniczenia przetwarzania,
6) wniesienia sprzeciwu wobec przetwarzania danych.

2. W przypadku wystąpienia któregokolwiek z powyższych żądań należy:

1) Zweryfikować, jakich danych przetwarzanych przez Hevelianum dotyczy sprawa i skierować ją do Działu, w którego kompetencji jest analiza wskazanych danych osobowych:
   a) w przypadku danych byłego pracownika – sprawę kieruje się do kadr,
   b) w przypadku danych podwykonawcy lub najemcy – sprawę kieruje się do Działu Administracji,
   c) w przypadku danych klienta, uczestnika wydarzeń w Hevelianum itp. sprawę kieruje się do odpowiedniego Działu,
   d) w przypadku żądania dotyczącego rozpowszechniania wizerunku osoby uwiecznionej na monitoringu – sprawę kieruje się do Działu Eksploatacji.
2) Ww. sprawy kieruje się jednocześnie do wiadomości Inspektora Ochrony Danych (iod@hevelianum.pl lub kontakt telefoniczny).
3) Po ustaleniu zakresu danych przetwarzanych przez Hevelianum należy upewnić się, czy żądanie pochodzi od właściciela danych.
4) W przypadku braku możliwości potwierdzenia tożsamości osoby, która wysłała żądanie należy skontaktować się z nią celem potwierdzenia tożsamości.
5) Następnie należy upewnić się, czy żądanie właściciela danych jest możliwe do spełnienia:
   a) w przypadku żądania dostępu do swoich danych, należy dane udostępnić w sposób, w jaki zostało złożone żądanie, a w przypadku dużej ilości danych, zwłaszcza danych szczególnych lub mogących uchodzić za wrażliwe,

skontaktować się z właścicielem danych celem ustalenia sposobu przekazania informacji,

b) w przypadku żądania kopii danych osobowych można udostępnić ksera dokumentów albo pisemną/e-mail informację z wypisanymi danymi, które przetwarzamy, po uprzednim ustaleniu z właścicielem danych sposobu przekazania kopii danych,
c) w przypadku żądania sprostowania danych, należy dane poprawić, jeżeli nie mamy uzasadnionych wątpliwości co do intencji właściciela danych,
d) w przypadku żądania ograniczenia przetwarzania, należy rozważyć zasadność żądania – jeżeli nie istnieje podstawa w przepisach prawa, ani dane nie są niezbędne Hevelianum z uwagi na realizowane zadania, zakres przetwarzanych danych należy ograniczyć,
e) w przypadku żądania usunięcia danych przetwarzanych na podstawie wcześniej udzielonej zgody (np. dane do celów kontaktowych, marketingowych, zgoda na przetwarzanie wizerunku w mediach społecznościowych i www, zgoda na przetwarzanie danych zawartych w CV do celów późniejszych rekrutacji), o ile dane nie są niezbędne, jako element dokumentacji z zakończonego postępowania rekrutacyjnego, itp., należy dane usunąć,
f) w przypadku żądania usunięcia danych przetwarzanych na podstawie innej niż zgoda, należy rozważyć podstawę przetwarzania danych – czy w dalszym ciągu ją mamy. W przypadku posiadania podstawy do przetwarzania należy przygotować odpowiedź wskazującą na podstawę oraz na okres czasu, przez jaki dane będą przechowywane. Odpowiedź przed wysłaniem do właściciela danych należy skonsultować z Inspektorem Ochrony Danych. W przypadku gdy podstawa do przetwarzania już nie istnieje, dane należy usunąć,
g) w przypadku wniesienia sprzeciwu wobec przetwarzania danych, należy zweryfikować podstawę do przetwarzania danych właściciela danych i sprawę przekazać do Inspektora Danych Osobowych.

6) Właściciela danych należy poinformować o podjętych działaniach, bez względu na ich wynik. W przypadku konieczności procedowania dłużej niż 7 dni, zasadnym będzie wysłanie informacji do właściciela danych o toczących się pracach nad realizacją jego żądania.
7) W razie jakichkolwiek wątpliwości należy skontaktować się z Inspektorem Ochrony Danych (iod@hevelianum.pl lub kontakt telefoniczny).

II. Postępowanie na wypadek utraty kontroli nad danymi osobowymi itp. Zdarzeń.

1. Niezwłocznie w przypadku stwierdzenia jakiegokolwiek zdarzenia, mogącego skutkować uratą kontroli przez Hevelianum nad przetwarzanymi danymi osobowymi, należy:

1) w pierwszej kolejności, zabezpieczyć dane osobowe,
2) skontaktować się z Inspektorem Danych Osobowych, który zobowiązany jest do podjęcia dalszych wymaganych prawem czynności (iod@hevelianum.pl

lub kontakt telefoniczny), oraz uzupełnić Opis Wydarzenia stanowiący załącznik nr 2 do niniejszej Instrukcji,
3) skontaktować się z osobami odpowiadającymi za dane osobowe, których dotyczy zdarzenie,
4) w przypadku zdarzenia związanego z systemami komputerowymi lub monitoringiem, dodatkowo skonsultować się z firmą odpowiedzialną za IT,
5) poinformować dyrekcję Hevelianum (Dyrektora, Zastępcę Dyrektora lub inną osobę upoważnioną do zastępowania Dyrektora Hevelianum podczas jego nieobecności).

2. Postępować zgodnie z uzgodnieniami z osobami odpowiedzialnymi za procedowanie zdarzenia, realizacją działań naprawczych i Inspektorem Ochrony Danych.

3. Szczegółowa procedura postępowania przy wybranych zdarzeniach przedstawiona została w tabeli, która stanowi załącznik nr 1 do Instrukcji.

Załącznik nr 1
Do Instrukcji postępowania
w przypadku wybranych zdarzeń
przy przetwarzaniu danych osobowych
w Hevelianum

Uchybienia lub zagrożenia	Uchybienie i zagrożenie nieświadome wewnętrzne i zewnętrzne	Postępowanie w przypadku uchybienia lub zagrożenia
W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych		
A1	Pomieszczenie, w którym przechowywane są dane osobowe pozostaje bez nadzoru	Należy zabezpieczyć dane osobowe oraz powiadomić IOD, który powiadamia ADO. IOD sporządza Protokół uchybienia.
A2	Dostęp do danych mają osoby nieupoważnione	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić IOD, który powiadamia ADO i sporządza Protokół uchybienia.
A3	Próba kradzieży danych osobowych w formie papierowej	Należy nie dopuścić do kradzieży danych osobowych i powiadomić IOD, który powinien zabezpieczyć dane i powiadomić ADO. IOD, powiadamia ADO i sporządza Protokół zagrożenia.
A4	Nieuprawniony dostęp do danych osobowych w formie papierowej	Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić IOD, który sporządza Protokół uchybienia i powiadamia ADO.
A5	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu	Należy powiadomić IOD, który powinien zabezpieczyć pomieszczenie, powiadomić ADO i sporządzić Protokół uchybienia.
A6	Próba włamania do pomieszczenia/budynku	Należy zabezpieczyć dowody i powiadomić IOD, który sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. IOD powiadamia ADO i sporządza protokół zagrożenia.
A7	Zniszczenie lub modyfikacja danych osobowych w formie papierowej	Należy zabezpieczyć dowody i powiadomić IOD, który sprawdza stan uszkodzeń, zabezpiecza dowody, powiadamia ADO oraz sporządza protokół zagrożenia.
A8	Wyrzucenie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie	Należy zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić IOD oraz przełożonych. IOD, sporządza Protokół zagrożenia.

W zakresie przetwarzania danych osobowych w systemie informatycznym		
B1	Komputer nie jest zabezpieczony hasłem	Należy zabezpieczyć dane osobowe oraz powiadomić ASI i IOD, który powiadamia ADO i sporządza Protokół uchybienia.
B2	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym	Należy powiadomić ASI i IOD, który we współpracy z ASI powinien sprawdzić system uwierzytelniania oraz sprawdzić, czy nie doszło do kradzieży lub zniszczenia danych. Na podstawie informacji uzyskanych od ASI, IOD powiadamia ADO i sporządza Protokół uchybienia.
B3	Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych	Należy nie dopuścić do kradzieży danych i powiadomić IOD i ASI. ASI w porozumieniu z IOD, powinien zabezpieczyć nośnik danych i powiadomić ADO. IOD, sporządza Protokół zagrożenia.
B4	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania	Należy zawiadomić ASI i IOD. ASI powinien przeprowadzić audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych i firewall. ASI przekazuje wynik audytu IOD, który powinien ocenić, czy nie doszło do utraty danych osobowych i w zależności od tego sporządzić protokół uchybienia lub zagrożenia. IOD powiadamia ADO.
B11	Brak aktywnego oprogramowania antywirusowego	Należy powiadomić ASI. ASI powinien zaktualizować lub nabyć oprogramowanie antywirusowe i powiadomić IOD, który powiadamia ADO i sporządza Protokół uchybienia.
B13	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym	Należy zabezpieczyć dowody i powiadomić ASI. ASI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia IOD, który powiadamia ADO i sporządza Protokół zagrożenia.

B14	Uszkodzenie komputerów, nośników danych	Należy powiadomić IOD, który w porozumieniu z ASI powinien ocenić w wyniku czego doszło do zniszczenia i przywrócić dane z kopii zapasowej. IOD powiadamia ADO i sporządza Protokół zagrożenia.
B15	Próba nieprawidłowej interwencji przy sprzęcie komputerowym	Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić ASI, który powiadamia IOD, który powiadamia ADO i sporządza Protokół uchybienia.
W zakresie zdarzeń niezależnych od działalności człowieka		
C16	Zdarzenia losowe (powódź, pożar, zalanie itp.)	IOD powoduje oszacowanie strat, powiadamia ADO i sporządza Protokół zagrożenia lub uchybienia.

Załącznik nr 2
Do Instrukcji postępowania
w przypadku wybranych zdarzeń
przy przetwarzaniu danych osobowych
w Hevelianum

OPIS ZDARZENIA

w związku z ryzykiem wystąpienia nieprawidłowości przy przetwarzaniu danych osobowych przez Hevelianum

wypełnia się w przypadku zdarzeń, w których istniało ryzyko, mogło dojść lub doszło do utraty kontroli przez Hevelianum nad przetwarzanymi danymi osobowymi na skutek takich zdarzeń jak: kradzież nośników danych (dokumentów lub sprzętu komputerowego), dostęp osób nieupoważnionych do danych, utrata danych (w tym na skutek działań zamierzonych, awarii, zdarzeń losowych takich jak pożar czy zalanie), czasowy brak dostępu do danych, ujawnienie danych osobie nieupoważnionej (w tym wysłanie korespondencji do niewłaściwego adresata), itp.

Data i godzina wystąpienia zdarzenia .....

Opis zdarzenia

.....
.....
.....
.....

Przyczyny powstania zdarzenia

.....
.....
.....

Zaistniałe skutki zdarzenia

.....
.....
.....

Podjęte działania naprawczo-zapobiegawcze

.....
.....
.....

Kontakt do osoby stwierdzającej zdarzenie.....

Informacje o innych osobach mogących mieć istotne informacje o zdarzeniu:

.....