

Choroba COVID-19 zaburza łańcuchy dostaw na całym świecie, wstrząsa giełdami i poprzez wprowadzane kwarantanny może prowadzić do zarządzanego ogólnie zamykania zakładów. Mimo, że sytuacja rozwija się bardzo dynamicznie i trudno jest dokonać rzetelnych prognoz, z perspektywy wszystkich przedsiębiorstw ważne jest, aby dzięki ukierunkowanemu zarządzaniu kryzysowemu przygotować się na wszelkie możliwe scenariusze i w ten sposób zapewnić sobie zaufanie swoich pracowników, partnerów biznesowych i klientów.

Jak zapewnić skuteczne zarządzanie kryzysowe? Decydującym czynnikiem jest rozsądne i efektywne działanie opierające się na następujących filarach:

- utworzenie sztabu kryzysowego
- dokonanie indywidualnej i uporządkowanej analizy ryzyka
- korzystanie ze sprawdzonych informacji i wiedzy eksperckiej

### I. Sztab kryzysowy:

Aby móc działać jak najskuteczniej i jak najszybciej, konieczne jest utworzenie sztabu kryzysowego. Do składu sztabu kryzysowego należy wyznaczyć (a nie tylko zaprosić) osoby odpowiedzialne ze wszystkich istotnych działów przedsiębiorstwa. Są to dział kadr, sprzedaży, marketingu i finansów. Aby móc odpowiednio reagować na szybki rozwój wypadków należy planować spotkania (telekonferencje) w regularnych i krótkich odstępach czasu.

Należy przydzielać kompetencje! Kto zaprasza? Kto może informować pracowników, klientów i/lub dostawców? Bezwzględnie należy unikać konfliktów interesów! Konflikt interesów występuje na przykład wtedy, gdy opracowanie konkretnego zagadnienia i jego weryfikacja przypisane są tylko jednej osobie.

Należy dokumentować przebieg spotkań kryzysowych! Stanowi to dowód podjęcia przez przedsiębiorcę wszelkich możliwych w danych okolicznościach kroków w celu zaradzenia kryzysowi. W dalszym czasie będą mogli Państwo dzięki temu wykazać zachowanie należytej staranności i tym samym uchronić się przed karami administracyjnymi lub roszczeniami regresowymi. Jednocześnie zapewniają Państwo, że nowi członkowie zespołu kryzysowego będą mogli kontynuować pracę swoich poprzedników w przypadku, gdy członkowie zespołu kryzysowego mieliby być nieobecni z powodu choroby.

### II. Analiza ryzyka:

Zespół kryzysowy powinien na początku swojej pracy przeprowadzić indywidualną analizę ryzyka. Analiza ryzyka pomaga rozpoznać i zidentyfikować w sposób usystematyzowany zadania do wykonania oraz czas, w którym powinny one być wykonane oraz ryzyka, które się z nimi wiążą.

W praktyce ugruntowało się opracowanie tabeli ryzyka. Nasi doradcy organizacyjni zalecają dokonanie klasyfikacji ryzyka na czterech poziomach (niski, średni, wysoki i bardzo wysoki). Oczywiście mogą Państwo przewidzieć również dodatkowe poziomy w swojej analizie, niemniej jednak z reguły czynią one analizę ryzyka znacznie bardziej złożoną. Proszę korzystać z prostych, dobrych i zrozumiałych struktur. Poniżej znajduje się przykładowa struktura tabeli ryzyka:

White paper: Zarządzanie kryzysem „COVID-19“

Poziom ryzyka	Kiedy występuje dany poziom?	Rozmiar i prawdopodobieństwo skutków w odniesieniu do Państwa przedsiębiorstwa	Działania, które przewidzieli Państwo na taki wypadek	Komunikacja z tym związana
niski	<ul style="list-style-type: none"> <li>ukryte zagrożenie</li> <li>brak przypadków zakażenia w przedsiębiorstwie oraz w sąsiedztwie</li> </ul>	skutki małe lub nieistotne, lecz wysokie prawdopodobieństwo ich wystąpienia	Działania prewencyjne, np. <ul style="list-style-type: none"> <li>plany higieny</li> <li>nabycie środków dezynfekcyjnych</li> <li>zalecenie odroczenia podróży służbowych oraz uczestnictwa w większych wydarzeniach</li> <li>przygotowanie infrastruktury IT w celu umożliwienia pracy zdalnej</li> </ul>	<ul style="list-style-type: none"> <li>szkolenia z zakresu higieny dla pracowników</li> <li>rozwieszenie ulotek informacyjnych</li> </ul>
średni	przypadki podejrzeń zakażeń lub zakażeń w bezpośrednim pobliżu przedsiębiorstwa lub jego pracowników	skutki dostrzegalne, rosnące prawdopodobieństwo w związku z rozprzestrzenianiem się wirusa wśród społeczeństwa	<ul style="list-style-type: none"> <li>zakaz podróży służbowych</li> <li>przygotowanie kryzysowego planu dot. zatrudnienia: przestrzenna / czasowa separacja zmian / zespołów / grup</li> <li>szczególna prewencja obejmującą personel kluczowy</li> <li>przygotowanie kryzysowego planu IT</li> <li>odwołanie organizowanych wydarzeń i eventów</li> </ul>	<ul style="list-style-type: none"> <li>pouczenie pracowników o rozprzestrzenianiu się i zagrożeniu zakażeniem</li> <li>apel w sprawie ochrony osób słabszych</li> <li>zobowiązanie do stosowania wszelkich środków prewencyjnych</li> </ul>
wysoki	przypadki podejrzeń zakażeń lub zakażeń w przedsiębiorstwie. Zamknięcie działów lub pojedynczych jednostek, które mogą jednak zostać zastąpione	skutki istotne – niskie prawdopodobieństwo (należy regularnie dokonywać nowej oceny)	<ul style="list-style-type: none"> <li>zarządzenie pracy w formie Home Office</li> <li>wdrożenie kryzysowych planów dot. zatrudnienia i IT</li> <li>zaciągnięcie informacji odnośnie możliwości uzyskania pomocy publicznej i innych finansowych środków stabilizujących</li> </ul>	<ul style="list-style-type: none"> <li>komunikacja ze wszystkimi istotnymi udziałowcami / akcjonariuszami</li> </ul>
bardzo wysoki	zaprzeszczenie produkcji lub jej części, których nie można zastąpić	skutki istotne z punktu widzenia istnienia przedsiębiorstwa, bardzo niskie prawdopodobieństwo (należy regularnie dokonywać nowej oceny)	<ul style="list-style-type: none"> <li>skorzystanie z pomocy publicznej, ubezpieczeń</li> <li>działania dotyczące zatrudnienia</li> </ul>	<ul style="list-style-type: none"> <li>komunikacja ze wszystkimi istotnymi udziałowcami / akcjonariuszami</li> <li>ewentualnie komunikacja z prasą</li> </ul>

Uwaga: Wskazane środki muszą być określone uwzględniając specyfikę danego przedsiębiorstwa i mają jedynie charakter przykładowy

### III. Wiedza – proszę korzystać z wiedzy ekspertów, oficjalnych ogłoszeń dokonywanych przez instytucje publiczne itd.

W sytuacji kryzysowej proszę korzystać ze sprawdzonych źródeł informacji takich jak

- oficjalne ogłoszenia dokonywane przez instytucje publiczne jak np. Rząd Federalny, Kraje Związkowe, zalecenia ze strony urzędów na poziomie federalnym i związkowym itd.
- wiedza fachowa Państwa pracowników / doradców zewnętrznych (np. inspektorów ochrony danych osobowych, administratorów systemu informatycznego) oraz
- w razie potrzeby – zaciągnięcie w konkretnych przypadkach rad ekspertów.

Poniższe informacje mają na celu przedstawienie Państwu poszczególnych źródeł informacji i wiedzy, nie mają jednak sposób charakteru wyczerpującego. Szczególnie jeśli chodzi o wskazane źródła i ogłoszenia dokonywane przez instytucje publiczne wskazać należy, że codziennie dodawane są nowe informacje; staramy się regularnie aktualizować niniejsze zestawienie. Kwestie prawne mogą zostać w tym miejscu jedynie zasygnalizowane – w tym zakresie prosimy o konsultację z Państwa doradcami prawnymi. Informacje z zakresu prawa pracy znajdują Państwo [tutaj](#).

#### 1. Ogłoszenia ze strony oficjalnych instytucji – stan na dzień: 18 marca 2020 r.:

Republika Federalna Niemiec	
Federalny Urząd Ochrony Cywilnej i Pomocy w Sytuacjach Kryzysowych	poradnik <a href="#">Planowanie działalności zakładu na wypadek pandemii</a>
BfDI – Federalny Rzecznik Ochrony Danych i Bezpieczeństwa Informacji	<a href="#">Informacje z zakresu ochrony danych osobowych dotyczące przetwarzania danych osobowych przez pracodawców w związku z pandemią koronawirusa</a>
Nadzór nad ochroną danych – Badenia-Wirtembergia	Najczęściej zadawane pytania i odpowiedzi ( <a href="#">FAQ</a> ) dot. tematu koronawirusa
Federalne Ministerstwo Pracy i Spraw Społecznych	„Koronawirus: skutki w zakresie prawa pracy“ - najczęściej zadawane pytania i odpowiedzi ( <a href="#">FAQ</a> )

Unia Europejska i inne państwa Europy	
<b>Dania</b>	
Datatilsynet	<a href="https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/hvordan-er-det-med-gdpr-og-coronavirus/">https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/hvordan-er-det-med-gdpr-og-coronavirus/</a>
<b>Francja</b>	
CNIL - Commission Nationale de l'Informatique et des Libertés	<a href="#">Coronavirus (Covid-19) : les rappels de la CNIL sur la collecte de données personnelles</a>
<b>Finlandia</b>	
TT – Tietosuojavaltuutetun toimisto	<a href="https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuoja-ja-koronaviruksen-leviamisen-hillitseminen">https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuoja-ja-koronaviruksen-leviamisen-hillitseminen</a>
<b>Irlandia</b>	
DPC – Data Protection Commission	<a href="#">Data Protection and COVID-19</a>
<b>Włochy</b>	
Garante per la protezione dei dati personali	<a href="https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9282117">https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9282117</a>
<b>Islandia</b>	
PV – Persóna Vernd	<a href="https://www.personuvernd.is/personuvernd/frettir/covid-19-og-personuvernd">https://www.personuvernd.is/personuvernd/frettir/covid-19-og-personuvernd</a>
<b>Holandia</b>	
AP – Autoriteit Persoonsgegevens	<a href="https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-en-uitkering/mijn-zieke-werknemer">https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-en-uitkering/mijn-zieke-werknemer</a>
<b>Luksemburg</b>	
CNPD – Commission nationale pour la protection des données	<a href="https://cnpd.public.lu/fr/actualites/national/2020/03/coronavirus.html">https://cnpd.public.lu/fr/actualites/national/2020/03/coronavirus.html</a>

Polska	
UODO – Urząd Ochrony Danych Osobowych	<a href="https://uodo.gov.pl/pl/138/1456">https://uodo.gov.pl/pl/138/1456</a>
Wielka Brytania	
ICO – Information Commissioner’s Office	<a href="#">Data protection and coronavirus: what you need to know</a>
Węgry	
NAIH - A Nemzeti Adatvédelmi és Információszabadság Hatóság	<a href="https://naih.hu/files/NAIH_2020_2586.pdf">https://naih.hu/files/NAIH_2020_2586.pdf</a>

## 2. Informacje z zakresu ochrony danych osobowych – stan na dzień: 18 marca 2020 r.:

Kwestie ochrony danych osobowych są szczególnie istotne w odniesieniu do Państwa pracowników. Proszę zawsze przestrzegać zasady, zgodnie z którą nawet w sytuacjach kryzysowych pracownik pozostaje „panem swoich danych”. Jest to o tyle istotne, że ten kryzys będzie w dużej mierze dotyczył danych na temat zdrowia.

Pracownik co do zasady nie musi podawać pracodawcy żadnych konkretnych informacji o swoim zdrowiu. W przypadkach podejrzeń zakażenia może jednak powstać obowiązek przeprowadzenia badania lekarskiego przez organ służby zdrowia. W przypadku powrotu z podróży lub stwierdzenia choroby w osobistym otoczeniu pracownika może również powstać obowiązek udzielenia informacji na temat miejsca pobytu lub osób, z którymi miało się kontakt. Obowiązek ten ma na celu umożliwienie Państwu jako pracodawcy oceny zagrożenia dla zdrowia danej osoby i innych pracowników.

### Dopuszczalność przetwarzania danych osobowych dotyczących zdrowia zatrudnionych osób

Dopuszczalność przetwarzania danych osobowych dotyczących zdrowia pracowników wynika z art. 9 RODO, art. 88 RODO w zw. z § 26 ust. 3 BDSG (niemieckiej ustawy o ochronie danych osobowych). Zgodnie z tymi przepisami przetwarzanie danych wrażliwych, takich jak dane dotyczące zdrowia, jest dopuszczalne do celów związanych ze stosunkiem pracy, jeżeli, między innymi, jest niezbędne do wypełnienia zobowiązań prawnych pracodawcy wynikających z prawa pracy i nie istnieje powód, aby zakładać, że uzasadniony interes osoby, której dane dotyczą, polegający na wyłączeniu przetwarzania danych, jest w tym przypadku nadrzędny.

Obowiązkiem prawnym jest przestrzeganie postanowień § 618 ust. 1 BGB (niemiecki Kodeks cywilny) w zw. z § 3 ArbSchG (niemiecka ustawa o BHP). Zgodnie z ustawą o bezpieczeństwie i higienie pracy pracodawca jest co do zasady zobowiązany do oceny zagrożeń dla bezpieczeństwa i zdrowia swoich pracowników w miejscu pracy (tzw. ocena ryzyka) oraz do wyciągnięcia na tej podstawie odpowiednich wniosków.

Powyższe może prowadzić do powstania sytuacji spornej: z jednej strony pracodawca musi wypełniać swój obowiązek opieki, chroniąc pracowników przed zakażeniem, ale z drugiej strony nie może naruszać ochrony danych osobowych i praw osobistych pracowników.

To, czy dane działanie jest dopuszczalne czy nie, zależy w dużej mierze od kryterium konieczności. Oceniając konieczność przetwarzania danych należy wziąć pod uwagę sprzeczne interesy pracodawcy i pracownika. W ten sposób interes pracodawcy w przetwarzaniu musi być starannie wyważony z prawem osobistym pracownika. Ta raczej teoretyczna definicja ostatecznie stanowi, że interesy obu stron muszą być wyważone, powzięte środki muszą być adekwatne do zamierzonego celu oraz że nie są dostępne łagodniejsze a równie skuteczne środki.

Należy również przestrzegać zasad prawa ochrony danych osobowych wynikających z art. 5 RODO. W szczególności zasady uczciwości ("dobrej wiary") i przejrzystości zgodnie z art. 5 ust. 1 lit. a) RODO, jak również zasada minimalizacji danych zgodnie z art. 5 ust. 1 lit. c) RODO, mają szczególne znaczenie dla wyważenia interesów. Zgodnie z tymi zasadami przetwarzanie danych musi być przewidywalne dla osób, których dane dotyczą, muszą być one informowane o rodzaju i zakresie przetwarzania danych, a przetwarzanie danych musi być ograniczone do minimum niezbędnego do osiągnięcia zamierzonego

celu. Jeśli powyższe zasady zostaną prawidłowo wdrożone, będzie to miało pozytywny wpływ na wynik analizy konieczności przetwarzania.

### Co jest dozwolone a co nie?

Na tym etapie trudno jest to ostatecznie ocenić - wydarzenia rozwijają się i w tym momencie brak jest jednego spójnego stanowiska europejskich organów nadzorujących ochronę danych. W związku z tym w tej chwili można dokonać jedynie wstępnej oceny jak poniżej.

Działania dopuszczalne	Działania niedopuszczalne
Zbieranie informacji o tym, czy pracownik przebywał w regionie ryzyka, czy miał bezpośredni kontakt z osobą chorą, np. przeprowadzanie rozmów z osobami powracającymi z urlopu w celu ustalenia, czy przebywały one w regionie ryzyka.	Nie wolno mówić pracownikom, że dany pracownik wskazany z imienia i nazwiska zachorował na chorobę wywołaną wirusem, ponieważ wiedza o tej konkretnej chorobie pracownika może prowadzić do jego stygmatyzacji. Zamiast tego należy podjąć działania na poziomie działu, w którym on pracował, lub zespołu bez wskazywania jednak na konkretną osobę. Pracownicy mający bezpośredni kontakt z osobami zakażonymi powinni być ostrzeżeni i tymczasowo zwolnieni z obowiązku wykonywania pracy.
Na wniosek organów służby zdrowia: przekazywanie danych o pracownikach, którzy są chorzy; o pracownikach przebywających w regionach ryzyka lub mających kontakt z osobami zakażonymi.	Ogólne wypytywanie wszystkich pracowników na temat celów podróży, w szczególności bez konkretnego powodu lub w przypadku braku występowania podróży.
Przeprowadzanie dobrowolnej ankiety dotyczącej miejsc pobytu i objawów.	Ogólne wypytywanie wszystkich pracowników na temat ich stanu zdrowia (np. o objawach grypy).
W przypadku pozytywnego wyniku badania pracownika (przeprowadzonego przez oficjalną jednostkę) lub nawet w przypadku potwierdzonego kontaktu z osobą, która uzyskała wynik pozytywny, mogą być przetwarzane dane dotyczące danego pracownika, np. czas i tożsamość osób bliskich oraz podjęte środki (por. francuski nadzór nad ochroną danych).	Obowiązek informowania pracowników o wystąpieniu objawów u współpracownika (por. włoski nadzór nad ochroną danych).
Za zgodą pracownika: zebranie aktualnych prywatnych numerów telefonów komórkowych lub innych danych kontaktowych w celach informacyjnych na wypadek zamknięcia przedsiębiorstwa lub podobnych przypadków (zob. poradnik "Planowanie działalności zakładu na wypadek pandemii" wydany przez Federalny Urząd Ochrony Cywilnej i Pomocy w Sytuacjach Kryzysowych).	Obowiązkowy pomiar temperatury dla pracowników przy wejściu do pomieszczeń lub podejmowanie podobnych środków medycznych (np. wymazy z gardła do pobierania próbek śliny). Działanie te może być dopuszczalne w konkretnych przypadkach => jego podjęcia wymaga jednak starannego rozważenia interesów wszystkich zainteresowanych stron.

### 3. Ochrona danych i informacji – stan na dzień: 18 marca 2020 r.:

Proszę w sposób krytyczny weryfikować ryzyka związane z ochroną danych i informacji przy okazji podejmowania m.in. następujących działań:

Działanie	Uwagi
Home Office	instalacja VPN; korzystanie z urządzeń służbowych; dyrektywy pracy w Home Office / telepracy
Wideokonferencje i inne	Wybór dostawcy; ewentualna konieczność porozumienia w celu wykonania zlecenia
Blokady dostępu do danych w obszarach wrażliwych	Dopuszczalne? Konieczne? Możliwe?
Ograniczenia możliwości odwiedzin / wizyt	Dopuszczalne? Konieczne? Możliwe?

### 4. Informacje z zakresu prawa pracy – stan na dzień: 18 marca 2020 r.:

Informacje z zakresu prawa pracy opracowane przez prawników kancelarii TIGGES Rechtsanwälte znajdują Państwo [tutaj](#).

Oczywiście chętnie udzielimy Państwu wsparcia w pozostałym zakresie – w razie potrzeby prosimy o kontakt.

**Państwa zespół TIGGES DCO!**