

DECYZJA NR 328
KOMENDANTA GŁÓWNEGO POLICJI

z dnia 9 października 2023 r.

w sprawie narzędzia informatycznego BIG DATA

Na podstawie art. 20 ust. 1 i 1d ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2023 r. poz. 171, z późn. zm.¹⁾) postanawia się, co następuje:

Rozdział 1
Przepisy ogólne

§ 1. Decyzja określa:

- 1) przeznaczenie i sposób funkcjonowania narzędzia informatycznego BIG DATA, zwanego dalej „BIG DATA”;
- 2) użytkowników i rolę w BIG DATA;
- 3) podział zadań w zakresie administrowania i nadzoru nad przetwarzaniem informacji w BIG DATA;
- 4) procedury nadawania lub odbierania uprawnień dostępu do BIG DATA;
- 5) zasady sprawdzeń informacji w BIG DATA.

§ 2. Użyte w decyzji określenia i skróty oznaczają:

- 1) CBŚP – Centralne Biuro Śledcze Policji;
- 2) CBZC – Centralne Biuro Zwalczania Cyberprzestępczości;
- 3) KGP – Komendę Główną Policji;
- 4) KSP – Komendę Stołeczną Policji;
- 5) KWP – komendę wojewódzką Policji;
- 6) CBDC – token będący pieniądzem elektronicznym lub token będący e-pieniądzem w rozumieniu art. 3 ust. 1 pkt 7 rozporządzenia 2023/1114;
- 7) kryptowaluta – rodzaj kryptoaktywa w rozumieniu art. 3 ust. 1 pkt 5 rozporządzenia 2023/1114, przechowujący informację o stanie posiadania w umownych jednostkach, służący głównie jako środek płatniczy lub środek wymiany;
- 8) token użytkowy – token użytkowy w rozumieniu art. 3 ust. 1 pkt 9 rozporządzenia 2023/1114;
- 9) podmioty pozapolicyjne – organy władzy publicznej, w tym służby, uprawnione do uzyskiwania informacji z BIG DATA oraz do ich przetwarzania;
- 10) podmioty uprawnione – komórki organizacyjne służby kryminalnej, śledczej, spraw wewnętrznych, kontrterrorystycznej oraz zwalczania cyberprzestępczości Policji;
- 11) rozporządzenie 2023/1114 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (Dz. Urz. UE L 150 z 09.06.2023, str. 40).

Rozdział 2
Przeznaczenie i sposób funkcjonowania BIG DATA

§ 3. 1. BIG DATA jest narzędziem informatycznym przeznaczonym do analizy informacji przez:

- 1) podmioty uprawnione – w celu realizacji ustawowych zadań Policji w zakresie:
 - a) zapobiegania, rozpoznawania, ujawniania i wykrywania przestępstw lub przestępstw skarbowych,

¹⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2022 r. poz. 2600 oraz z 2023 r. poz. 185, 240, 289, 347, 535, 641, 1088 i 1860.

- b) ustalania metod popełniania przestępstw lub przestępstw skarbowych oraz wykrywania i zatrzymywania ich sprawców,
 - c) rozpoznawania zagrożeń terrorystycznych,
 - d) ratowania życia lub zdrowia ludzkiego,
 - e) wsparcia działań poszukiwawczych lub ratowniczych;
- 2) podmioty pozapolicyjne – w zakresie niezbędnym do realizacji ich ustawowych zadań, na zasadach określonych w porozumieniach zawartych z kierownikami tych podmiotów.

2. BIG DATA składa się z:

- 1) projektów;
- 2) repozytoriów centralnych;
- 3) zbiorów identyfikujących.

§ 4. 1. Projekt jest wyodrębnionym merytorycznie zbiorem informacji utworzonym przez operatora w celu realizacji konkretnej sprawy lub analizy zagadnienia tematycznego.

2. Projekty mogą posiadać status:

- 1) otwarty – w trakcie trwania analizy informacji zawartych w projekcie;
- 2) zawieszony – w przypadku czasowego wstrzymania analizy informacji zawartych w projekcie, na okres nie dłuższy niż 6 miesięcy;
- 3) zamknięty – w przypadku zakończenia analizy informacji zawartych w projekcie.

3. Decyzję o zmianie statusu projektu podejmuje operator lub jego bezpośredni przełożony, z zastrzeżeniem § 7 ust. 5 pkt 3 i ust. 8 pkt 4.

4. Projekty wraz z przetwarzanymi w nich informacjami usuwa się:

- 1) po upływie:
 - a) 3 lat od dnia utworzenia projektu,
 - b) 1 roku od dnia zawieszenia projektu,
 - c) 6 miesięcy od dnia zamknięcia projektu;
- 2) w przypadku braku zgodności z przeznaczeniem BIG DATA.

5. Na pisemny wniosek kierownika jednostki lub komórki organizacyjnej podmiotu uprawnionego lub podmiotu pozapolicyjnego, którego funkcjonariusz lub pracownik przetwarza informacje w projekcie, o którym mowa w ust. 4 pkt 1, kierownik komórki organizacyjnej KGP właściwej w sprawach wywiadu kryminalnego może podjąć decyzję o odstąpieniu od usunięcia projektu na okres 1 roku.

§ 5. 1. Repozytoria centralne są przeznaczone do sprawdzeń informacji w celu koordynacji działań podmiotów uprawnionych i pozapolicyjnych.

2. W repozytoriach centralnych przetwarza się niezawierające danych osobowych informacje dotyczące:

- 1) numerów rachunków bankowych prowadzonych przez bank lub inną instytucję finansową świadczącą usługi na terenie Rzeczypospolitej Polskiej lub poza jej granicami,
- 2) adresów i transakcji kryptowalut, tokenów użytkowych i CBDC
 - w zakresie wynikających z przepisów prawa powszechnie obowiązującego uprawnień Policji do przetwarzania tych informacji.

3. W skład BIG DATA wchodzi repozytoria centralne pod nazwą:

- 1) „Konta w zainteresowaniu”;
- 2) „Konta zagraniczne w zainteresowaniu”;
- 3) „Adresy kryptowalut w zainteresowaniu”;

4) „Transakcje kryptowalut w zainteresowaniu”.

4. Decyzję o umieszczeniu informacji w repozytorium centralnym podejmuje operator lub jego bezpośredni przełożony, z zastrzeżeniem § 12 ust. 4.

5. Informacje z repozytorium centralnego usuwa się po upływie 10 lat od dnia ich umieszczenia w tym repozytorium.

§ 6. 1. Zbiory identyfikujące są przeznaczone do przetwarzania niezawierających danych osobowych informacji w celu identyfikacji podmiotów niebędących osobami fizycznymi, świadczących na terenie Rzeczypospolitej Polskiej lub poza jej granicami usługi związane z operacjami na kryptowalutach, tokenach użytkowych oraz CBDC, w tym usługi ich kupna, sprzedaży albo wymiany na towary lub usługi, w zakresie wynikających z przepisów prawa powszechnie obowiązującego uprawnień Policji do przetwarzania tych informacji.

2. W skład BIG DATA wchodzi zbiory identyfikujące pod nazwą:

- 1) „Coinfirm”;
- 2) „DataWalk”;
- 3) „BIG DATA nazwa”.

3. Decyzję o umieszczeniu informacji w zbiorach identyfikujących pod nazwą „Coinfirm” i „DataWalk” podejmuje Centralny Administrator Merytoryczny.

4. Decyzję o umieszczeniu informacji w zbiorze identyfikującym pod nazwą „BIG DATA nazwa” podejmuje operator lub jego bezpośredni przełożony.

5. Informacje ze zbioru identyfikującego usuwa się po upływie 10 lat od dnia ich umieszczenia w tym zbiorze.

Rozdział 3 **Użytkownicy i role w BIG DATA**

§ 7. 1. Użytkownikami BIG DATA mogą być:

- 1) funkcjonariusze pełniący służbę lub pracownicy Policji zatrudnieni w podmiotach uprawnionych – w celu realizacji zadań określonych w § 3 ust. 1 pkt 1;
- 2) funkcjonariusze pełniący służbę lub pracownicy Policji zatrudnieni w Akademii Policji w Szczytnie, szkołach policyjnych lub ośrodkach szkolenia Policji – w celach szkoleniowych;
- 3) funkcjonariusze pełniący służbę lub pracownicy podmiotów pozapolicyjnych zatrudnieni w nich – w zakresie wskazanym w § 3 ust. 1 pkt 2;
- 4) funkcjonariusze pełniący służbę lub pracownicy podmiotów pozapolicyjnych zatrudnieni w szkołach lub ośrodkach szkolenia tych podmiotów – w celach szkoleniowych.

2. W BIG DATA wyróżnia się następujące role:

- 1) Centralny Administrator Merytoryczny;
- 2) Lokalny Koordynator Merytoryczny;
- 3) operator.

3. Kierownik komórki organizacyjnej KGP właściwej w sprawach wywiadu kryminalnego wyznacza Centralnego Administratora Merytorycznego spośród funkcjonariuszy pełniących służbę lub pracowników Policji zatrudnionych w tej komórce organizacyjnej.

4. Centralny Administrator Merytoryczny posiada uprawnienia dostępu do wszystkich informacji przetwarzanych w BIG DATA.

5. Do zadań Centralnego Administratora Merytorycznego należy:

- 1) sprawowanie nadzoru nad przetwarzaniem informacji przez użytkowników zgodnie z:
 - a) przeznaczeniem BIG DATA,

b) posiadanymi przez nich uprawnieniami;

- 2) aktualizacja informacji niezbędnych do prawidłowego funkcjonowania BIG DATA;
- 3) weryfikacja, zmiana statusu oraz usuwanie projektów wraz z przetwarzanymi w nich informacjami;
- 4) usuwanie informacji z repozytoriów centralnych i zbiorów identyfikujących;
- 5) realizacja procesu szkoleniowego i doskonalenia zawodowego użytkowników w zakresie przetwarzania informacji w BIG DATA, w tym wspieranie osób, o których mowa w ust. 1 pkt 2 i 4;
- 6) przygotowywanie propozycji zmian w zakresie nowych rozwiązań, funkcjonalności oraz innych modyfikacji w BIG DATA;
- 7) zgłaszanie dyżurnemu komórki organizacyjnej KGP właściwej w sprawach łączności i informatyki nieprawidłowości w funkcjonowaniu BIG DATA, po wyeliminowaniu błędów użytkowników.

6. Kierownik komórki organizacyjnej KGP, CBŚP, CBZC, KWP lub KSP właściwej w sprawach wywiadu kryminalnego albo komórki organizacyjnej Biura Spraw Wewnętrznych Policji właściwej w sprawach wsparcia operacyjnego wyznacza Lokalnego Koordynatora Merytorycznego spośród funkcjonariuszy pełniących służbę lub pracowników Policji zatrudnionych w tych komórkach organizacyjnych.

7. Lokalny Koordynator Merytoryczny posiada uprawnienia dostępu do wszystkich informacji przetwarzanych w BIG DATA w komórce organizacyjnej, w której pełni służbę lub jest zatrudniony, oraz w komórkach organizacyjnych nadzorowanych przez tę komórkę.

8. Do zadań Lokalnego Koordynatora Merytorycznego należy:

- 1) bezpośrednie koordynowanie przetwarzania informacji przez użytkowników w komórkach organizacyjnych, o których mowa w ust. 7, zgodnie z:
 - a) przeznaczeniem BIG DATA,
 - b) posiadanymi przez nich uprawnieniami;
- 2) nadzór nad uprawnieniami nadanymi użytkownikom w komórkach organizacyjnych, o których mowa w ust. 7;
- 3) zgłaszanie potrzeb w zakresie aktualizacji informacji niezbędnych do prawidłowego funkcjonowania BIG DATA;
- 4) weryfikacja, zmiana statusu oraz usuwanie projektów wraz z przetwarzanymi w nich informacjami w komórkach organizacyjnych, o których mowa w ust. 7;
- 5) realizacja procesu szkoleniowego i doskonalenia zawodowego użytkowników w zakresie przetwarzania informacji w BIG DATA, w tym wspieranie Centralnego Administratora Merytorycznego w wykonywaniu zadania, o którym mowa w ust. 5 pkt 5;
- 6) zgłaszanie Centralnemu Administratorowi Merytorycznemu propozycji zmian w zakresie nowych rozwiązań, funkcjonalności oraz innych modyfikacji w BIG DATA;
- 7) zgłaszanie Centralnemu Administratorowi Merytorycznemu nieprawidłowości w funkcjonowaniu BIG DATA, po wyeliminowaniu błędów użytkowników.

9. Kierownik podmiotu uprawnionego wyznacza operatora spośród funkcjonariuszy pełniących służbę lub pracowników Policji zatrudnionych w tym podmiocie.

10. Operator może nadać lub odebrać innemu użytkownikowi uprawnienia dostępu do projektu, w którym przetwarza informacje, z zastrzeżeniem ust. 4 i 7.

11. Do zadań operatora należy:

- 1) wykorzystywanie BIG DATA zgodnie z przeznaczeniem;
- 2) nadawanie statusu projektu, o którym mowa w § 4 ust. 2;
- 3) usuwanie projektów w przypadkach wskazanych w § 4 ust. 4 i 5;
- 4) wykonywanie zadań zleconych przez Centralnego Administratora Merytorycznego i Lokalnego Koordynatora Merytorycznego;

- 5) informowanie Lokalnego Administratora Merytorycznego o nieprawidłowościach w funkcjonowaniu BIG DATA.

Rozdział 4

Administrowanie i nadzór nad przetwarzaniem informacji w BIG DATA

§ 8. 1. Kierownika komórki organizacyjnej KGP właściwej w sprawach wywiadu kryminalnego upoważnia się do:

- 1) pełnienia funkcji administratora w odniesieniu do informacji przetwarzanych w BIG DATA;
- 2) wydawania wytycznych dotyczących szczegółowego sposobu wykonywania czynności służbowych związanych z przetwarzaniem informacji w BIG DATA;
- 3) akceptowania zmian w zakresie nowych rozwiązań, funkcjonalności oraz innych modyfikacji w BIG DATA;
- 4) sprawowania nadzoru nad jakością i aktualnością informacji przetwarzanych w BIG DATA oraz dokonywania bieżącej weryfikacji pod względem ich zgodności z przeznaczeniem BIG DATA.

2. Kierownik komórki organizacyjnej KGP właściwej w sprawach wywiadu kryminalnego sprawuje nadzór, o którym mowa w ust. 1 pkt 4, poprzez kontrolę dostępu i analizowanie operacji przetwarzania informacji w BIG DATA.

3. W przypadku stwierdzonych uchybień w przetwarzaniu informacji w BIG DATA kierownik komórki organizacyjnej KGP właściwej w sprawach wywiadu kryminalnego wydaje zalecenia lub wytyczne w celu ich usunięcia.

§ 9. 1. Kierownik komórki organizacyjnej KGP właściwej w sprawach wywiadu kryminalnego jest odpowiedzialny za jakość informacji przetwarzanych w BIG DATA.

2. Kierownik komórki organizacyjnej KGP właściwej w sprawach łączności i informatyki jest odpowiedzialny za zapewnienie bezawaryjnego funkcjonowania BIG DATA pod względem technicznym oraz bezpieczeństwa teleinformatycznego.

Rozdział 5

Procedura nadawania lub odbierania uprawnień dostępu do BIG DATA

§ 10. 1. Uprawnienia do przetwarzania informacji w BIG DATA, zwane dalej „uprawnieniami dostępu do BIG DATA”, mogą być nadane lub odebrane na pisemny wniosek kierownika podmiotu uprawnionego lub kierownika jednostki organizacyjnej Policji, o której mowa w § 7 ust. 1 pkt 2.

2. Kierownik, o którym mowa w ust. 1, przesyła wniosek w dwóch egzemplarzach do kierownika komórki organizacyjnej KGP właściwej w sprawach wywiadu kryminalnego, w celu jego zatwierdzenia.

3. Wniosek zatwierdza kierownik komórki organizacyjnej KGP właściwej w sprawach wywiadu kryminalnego lub osoba przez niego upoważniona.

4. Kierownik komórki organizacyjnej KGP właściwej w sprawach wywiadu kryminalnego zwraca kierownikowi, o którym mowa w ust. 1, wniosek niezatwierdzony z powodu braków formalnych lub oceniony jako nieuzasadniony.

5. Kierownik komórki organizacyjnej KGP właściwej w sprawach wywiadu kryminalnego przesyła zatwierdzony wniosek kierownikowi komórki organizacyjnej KGP właściwej w sprawach łączności i informatyki, w celu niezwłocznej realizacji.

6. Po nadaniu lub odebraniu uprawnień dostępu do BIG DATA kierownik komórki organizacyjnej KGP właściwej w sprawach łączności i informatyki odsyła kierownikowi, o którym mowa w ust. 1, egzemplarz nr 1 wniosku.

7. Wzór wniosku o nadanie lub odebranie uprawnień dostępu do BIG DATA określa załącznik do decyzji.

§ 11. 1. Kierownik, o którym mowa w § 10 ust. 1:

- 1) dokonuje bieżącej weryfikacji uprawnień dostępu do BIG DATA nadanych funkcjonariuszowi lub pracownikowi Policji w zakresie:
 - a) zgodności posiadanych uprawnień dostępu do BIG DATA z realizowanymi zadaniami służbowymi,

- b) aktualności danych zawartych we wniosku, o którym mowa w § 10 ust. 1;
 - 2) niezwłocznie składa wniosek o odebranie uprawnień dostępu do BIG DATA, jeżeli funkcjonariusz lub pracownik Policji:
 - a) został zawieszony w czynnościach służbowych lub w pełnieniu obowiązków,
 - b) został przeniesiony do pełnienia służby lub wykonywania pracy w innej jednostce lub komórce organizacyjnej Policji,
 - c) zmarł;
 - 3) składa wniosek o odebranie uprawnień dostępu do BIG DATA przed podpisaniem karty obiegowej w związku ze zwolnieniem funkcjonariusza ze służby lub rozwiązaniem umowy o pracę zawartej z pracownikiem Policji.
2. Kierownik komórki organizacyjnej KGP właściwej w sprawach łączności i informatyki zwraca do weryfikacji wniosek, o którym mowa w § 10 ust. 1, oraz informuje kierownika komórki organizacyjnej KGP właściwej w sprawach wywiadu kryminalnego w przypadku stwierdzenia:
- 1) posiadania przez funkcjonariusza lub pracownika Policji więcej niż jednego identyfikatora kadrowego;
 - 2) posiadania tego samego identyfikatora kadrowego przez więcej niż jednego funkcjonariusza lub pracownika Policji.
3. W przypadku, o którym mowa w ust. 2 pkt 1, kierownik komórki organizacyjnej KGP właściwej w sprawach łączności i informatyki informuje również kierownika komórki organizacyjnej KGP właściwej w sprawach kadrowych.
4. Kierownik, o którym mowa w § 10 ust. 1, lub osoba przez niego upoważniona, przynajmniej raz w roku przeprowadza weryfikację uprawnień dostępu do BIG DATA nadanych w podmiocie uprawnionym lub jednostce organizacyjnej Policji, o której mowa w § 7 ust. 1 pkt 2.

Rozdział 6

Zasady sprawdzeń informacji w BIG DATA

- § 12. 1. Sprawdzenia informacji w BIG DATA dokonuje się w repozytoriach centralnych:**
- 1) zgodnie z przeznaczeniem BIG DATA;
 - 2) w związku z wymianą informacji z podmiotami pozapolicyjnymi;
 - 3) w związku z wymianą informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi.
2. Sprawdzenia dla podmiotów, o których mowa w ust. 1 pkt 2, wykonują właściwe miejscowo komórki organizacyjne KGP, KWP lub KSP, właściwe w sprawach wywiadu kryminalnego.
3. Sprawdzenia dla podmiotów, o których mowa w ust. 1 pkt 3, wykonują:
- 1) komórka organizacyjna KGP właściwa w sprawach wywiadu kryminalnego – na podstawie wniosku komórki organizacyjnej KGP pełniącej funkcję punktu kontaktowego do wymiany informacji, wyznaczonej na podstawie art. 4 ust. 1 ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz. U. z 2023 r. poz. 783);
 - 2) komórki organizacyjne KGP, CBZC, CBŚP, KWP lub KSP, właściwe w sprawach wywiadu kryminalnego – na podstawie wniosku właściwej miejscowo komórki organizacyjnej Policji uprawnionej do bezpośredniej wymiany informacji w ramach międzynarodowej współpracy Policji.
4. Informację podlegającą sprawdzeniu, o którym mowa w ust. 1, dodaje się do repozytorium centralnego.

Rozdział 7
Przepis końcowy

§ 13. Decyzja wchodzi w życie po upływie 7 dni od dnia podpisania.



Komendant Główny Policji

gen. insp. Jarosław SZYMCZYK

[Faint, illegible handwritten text]

[Faint, illegible handwritten text]

Załącznik do decyzji nr 328
Komendanta Głównego Policji
z dnia 9.10.2023 r.

Pieczęć nagłówkowa jednostki organizacyjnej
podmiotu uprawnionego⁴

Miejscowość,data

ZATWIERDZAM
(Dyrektor/Zastępca Dyrektora BWiIK KGP/osoba upoważniona)

Egz. Nr

Dyrektor
Biura Wywiadu i Informacji Kryminalnych KGP
w Warszawie

Wniosek o nadanie/odebranie¹ uprawnień dostępu do BIG DATA

ID KADRA	PESEL	IMIĘ I NAZWISKO
Jednostka/komórka organizacyjna podmiotu uprawnionego ⁴ miejsca pracy/służby		Praca na rzecz jednostki
Kod jednostki/komórki organizacyjnej podmiotu uprawnionego ⁴ miejsca pracy/służby		Kod jednostki - praca na rzecz

Lp.	ROLA 1 ² Centralny Administrator Merytoryczny	ROLA 2 ³ Lokalny Koordynator Merytoryczny	ROLA 3 operator
1	☐	☐	☐

.....
pieczęć i podpis bezpośredniego przełożonego użytkownika

Sporządził: imię, nazwisko, nr tel.

Wyk. w 2 egz.

Egz. nr 1 – adresat/nadawca po nadaniu uprawnień zwrot do

Egz. nr 2 – Administrator użytkowników z Blii KGP

¹ Niepotrzebne skreślić.

² Uprawnienia wyłącznie dla użytkowników z BWiIK KGP.

³ Uprawnienie wyłącznie dla użytkowników z KGP, CBŚP, CBZC, KWP lub KSP właściwej w sprawach wywiadu kryminalnego albo komórki organizacyjnej BSWP właściwej w sprawach wsparcia operacyjnego.

⁴ Lub jednostki organizacyjnej Policji, o której mowa w § 7 ust. 1 pkt 2 decyzji.

Data nadania/odebrania uprawnień oraz podpis administratora użytkowników KGP

Uzasadnienie

Potrzeba wydania decyzji Komendanta Głównego Policji wynika z faktu wdrożenia narzędzia informatycznego BIG DATA, służącego do analizy informacji ze szczególnym uwzględnieniem dużych zbiorów danych, przepływów finansowych, środków pieniężnych i kryptowalut.

Informacje, które będą przetwarzane w BIG DATA będą podlegać ochronie na podstawie przepisów *ustawy z dnia 6 kwietnia 1990 r. o Policji* (Dz. U. z 2023 r. poz. 171, z późn. zm.), a w przypadku danych osobowych – również na podstawie przepisów *ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości* (Dz. U. z 2023 r. poz. 1206).

Dostawa i uruchomienie narzędzia informatycznego BIG DATA nastąpi na podstawie umowy nr 129/208/Błil/21/KK/FBW dot. „Budowy systemu pod nazwą BIG DATA” zawartej w Warszawie w dniu 15 lipca 2022 r.

W rozdziale 1 wskazano zakres regulacji decyzji, a także przedstawiono definicje użytych w decyzji określeń i skrótów. W szczególności wskazano, że podmiotami uprawnionymi w rozumieniu przepisów decyzji są komórki organizacyjne służby kryminalnej, śledczej, spraw wewnętrznych, kontrterrorystycznej oraz zwalczania cyberprzestępczości Policji, zaś podmiotami pozapolicyjnymi – organy władzy publicznej, w tym służby, uprawnione do uzyskiwania informacji z BIG DATA oraz do ich przetwarzania.

W Rozdziale 2 opisano przeznaczenie i sposób funkcjonowania BIG DATA. Wskazano cele przetwarzania informacji uzyskanych przez podmioty uprawnione i pozapolicyjne. Określono przeznaczenie i zasady przetwarzania informacji w projektach, repozytoriach centralnych oraz zbiorach identyfikujących.

W Rozdziale 3 wskazano kto może zostać użytkownikiem BIG DATA. Określono również role (Centralny Administrator Merytoryczny, Lokalny Koordynator Merytoryczny oraz operator) i zadania użytkowników.

Rozdział 4 precyzuje zagadnienia administracji i nadzoru nad przetwarzaniem informacji w BIG DATA. Wskazuje kierowników komórek organizacyjnych KGP, którzy w imieniu Komendanta Głównego Policji pełnią funkcję administratora w odniesieniu do informacji przetwarzanych w BIG DATA, a także odpowiadają za zapewnienie bezawaryjnego funkcjonowania BIG DATA pod względem technicznym oraz bezpieczeństwa.

Rozdział 5 reguluje procedurę nadawania lub odbierania uprawnień dostępu do BIG DATA. Zgodnie z § 10 uprawnienia te nadawane będą na podstawie wniosków, których wzór określa załącznik nr 1 do decyzji. Wnioski te będą zatwierdzane przez kierownika komórki organizacyjnej KGP właściwej w sprawach wywiadu kryminalnego i realizowane przez komórkę organizacyjną KGP właściwą w sprawach łączności i informatyki. Nadzór nad weryfikacją uprawnień, zgodnie z § 11 sprawują kierownicy jednostek lub komórek organizacyjnych podmiotów uprawnionych lub osoby przez nich upoważnione, a w przypadku uprawnień nadanych funkcjonariuszom pełniącym służbę lub pracownikom Policji zatrudnionym w Akademii Policji w Szczytnie, szkołach policyjnych lub ośrodkach szkolenia Policji – kierownicy tych jednostek organizacyjnych Policji lub osoby przez nich upoważnione.

Rozdział 6 określa zasady sprawdzeń informacji w BIG DATA w repozytoriach centralnych. § 12 wskazuje komórki organizacyjne Policji wykonujące sprawdzenia w BIG DATA dla podmiotów pozapolicyjnych w związku z wymianą informacji.