

**Pierwsza konfiguracja za pomocą usługi
Intune
Smartfon i tablet
w DB Workplace Mobile**

(system operacyjny Android 15 i nowsze)
15 kwietnia 2026

Spis treści

1 Ważna aplikacja: aplikacja DB MOBIL Info	5
2 Rozpakowywanie smartfona/tabletu	6
2.1 Dwa sposoby odbioru smartfona/tabletu	6
2.2 Czy sam zamówiłeś swój nowy smartfon/tablet i go otrzymałeś?	6
2.3 Sprawdzanie zawartości przesyłki	6
2.4 Krótki przewodnik po konfiguracji smartfona/tabletu	6
3 Warunek wstępny: użytkownik DB	8
3.1 Już należysz do grupy DB i jesteś użytkownikiem bazy danych	8
3.2 Jesteś nowy w grupie, wymagane konto: użytkownik DB	8
4 Wstępna konfiguracja dla urządzeń Samsung/HMD	9
4.1 Wkładanie karty SIM	9
4.2 PIN karty SIM	9
4.3 Ustawianie blokady ekranu	10
4.4 Konfiguracja Wi-Fi	10
4.5 Konfiguracja Wi-Fi w budynkach DB	12
4.6 Aktywacja urządzenia – utworzenie tymczasowej legitymacji pracownika DB (TAP)	13
4.7 Utwórz tymczasową legitymację pracownika DB dla współpracownika	16
4.8 Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB (TAP)	18
4.9 Konfiguracja dostępu do wszystkich aplikacji i stron internetowych DB	20
4.10 Aplikacje DB	21
4.11 Zmiana blokady ekranu	21
4.12 Start: „Zaloguj się na smartfonie/tablecie	22
4.13 Wskazówki dotyczące codziennego uruchamiania	23
5 Treści służbowe i prywatne	24
5.1 Rozróżnienie między użyciem służbowym a prywatnym	24
5.2 Pobieranie aplikacji z bazy danych	26
5.3 Zarządzanie elementami na ekranie głównym	26
5.4 Start: Oddzielanie aplikacji prywatnych od służbowych + grupowanie aplikacji	28
6 Dalsze ustawienia	29
6.1 System operacyjny	29
6.2 Szybki dostęp/Centrum sterowania	29

6.3 Take-Off: Zarządzanie aplikacjami na ekranie głównym	31
6.3.1 Tworzenie folderu (grupy)	31
6.3.2 Zmiana nazwy folderu (grupy)	31
6.3.3 Przenoszenie aplikacji/folderów	31
6.3.4 Przenoszenie aplikacji na ekran główny	31
6.3.5 Tablet Samsung/HMD:	31
6.4 Połącz się z Internetem	32
6.4.1 Wi-Fi DB	32
6.4.2 Publiczne Wi-Fi	32
6.4.3 Informacje o transmisji danych – limit danych	32
6.4.4 Twoja umowa z Vodafone – Elfe (elektroniczny rachunek telekomunikacyjny)	32
6.4.5 Wyłączanie ostrzeżenia o danych	33
6.4.6 Tryb offline (tryb samolotowy)	36
6.5 F5 Access – Nawiązanie połączenia VPN	37
6.5.1 Konfiguracja połączenia VPN	37
6.6 Start: certyfikaty i połączenie VPN	39
6.7 Wydłużanie czasu pracy baterii	40
6.8 Wyłącz identyfikator reklamowy	40
7 Najważniejsze aplikacje na początek	41
7.1 Pobierz nowe aplikacje DB	41
7.2 Aplikacja DB MOBIL Info	41
7.2.1 Powiadomienia push	43
7.2.2 Skanowanie kodów QR	44
7.3 Outlook	45
7.3.1 Konfiguracja programu Outlook / Utworzenie konta e-mail / Konfiguracja szyfrowania wiadomości e-mail	45
7.3.2 Konfiguracja podpisu e-mail	47
7.3.3 Synchronizacja poczty e-mail – wszystkie wiadomości zawsze aktualne	49
7.3.4 Tworzenie nowych kontaktów w programie Outlook	49
7.3.5 Synchronizacja kontaktów w programie Outlook	49
7.4 Aplikacja MS Defender – należy ją otworzyć	50
7.4.1 Konfiguracja aplikacji MS Defender	50
7.4.2 Przyznawanie uprawnień	53
7.5 DB M 365	56
7.6 Aplikacja Microsoft Authenticator do uwierzytelniania	57
7.7 Podsumowanie: aplikacje bazodanowe	59

8 Tworzenie kopii zapasowych danych	60
8.1 Tworzenie kopii zapasowej danych służbowych w usłudze OneDrive	60
8.2 Konfiguracja OneDrive	60
8.2.1 Android 15	61
8.2.2 Android 16	62
8.3 Tworzenie kopii zapasowej zdjęć	63
8.4 Tworzenie kopii zapasowej plików PDF	66
8.4.1 Zapisywanie plików PDF bezpośrednio w OneDrive	68
8.5 Tworzenie kopii zapasowej kontaktów w usłudze OneDrive	69
8.6 Importowanie kontaktów z OneDrive	71
8.7 Tworzenie kopii zapasowej kontaktów za pośrednictwem programu Outlook	73
8.8 Tworzenie kopii zapasowej haseł	73
8.9 Tworzenie kopii zapasowej danych osobowych	74
8.10 Start: Gdzie są Twoje zdjęcia, pliki i dokumenty?	74
9 Ochrona danych i informacje o użytkowaniu	76
9.1 Take-Off: Aspekty bezpieczeństwa	78
10 Zapomniane hasło, zwrot urządzenia	79
10.1 Zapomniane lub zmiana hasła użytkownika DB	79
10.2 Pomoc za pośrednictwem aplikacji IT ServiceDesk	81
10.3 Zgubiłeś smartfon lub tablet?	82
10.4 Uszkodzony smartfon/tablet	83
10.5 Zwracasz smartfon/tablet?	83
10.6 Gratulacje!	84

1 Ważna aplikacja: aplikacja DB MOBIL Info

W tym przewodniku wyjaśniono, jak skonfigurować smartfon/tablet. Zawiera on również przegląd wszystkich tematów związanych z Twoim smartfonem/tabletem DB.



Najważniejszą aplikacją do wstępnej konfiguracji jest **aplikacja DB MOBIL Info!**

Znajdziesz tam wszystkie niezbędne informacje dotyczące swojego smartfona/tabletu, takie jak:

- Poradniki dotyczące konfiguracji i renowacji smartfona/tabletu
- Przydatne linki dotyczące pracy w świecie baz danych
- W tym miejscu będziesz otrzymywać powiadomienia o wszystkich ważnych sprawach dotyczących Twojego urządzenia

Zajrzyj więc i bądź na bieżąco!

Uwaga: Jeśli Twój smartfon/tablet nie jest jeszcze skonfigurowany, aplikacja DB MOBIL jest już zainstalowana na Twoim urządzeniu!

2 Rozpakowywanie smartfona/tabletu

2.1 Dwa sposoby odbioru smartfona/tabletu

Istnieją dwa sposoby odbioru smartfona/tabletu:

- Poprzez zamówienie w sklepie internetowym
- > Przejdź do sekcji 2.2 Czy samodzielnie zamówiłeś nowy smartfon/tablet i już go otrzymałeś?
- A może otrzymałeś urządzenie za pośrednictwem swojego centrum kosztów lub opiekuna umowy (komórkowej)
- > Przejdź do sekcji 2.3 Sprawdzanie zawartości przesyłki

2.2 Czy samodzielnie zamówiłeś nowy smartfon/tablet i już go otrzymałeś?

Najpierw sprawdź, czy na paczce widnieje Twoje imię i nazwisko oraz czy otrzymałeś właściwą przesyłkę. Porównaj ją z zamówieniem. Jeśli dane nie zgadzają się, skontaktuj się ze swoim centrum kosztów lub osobą odpowiedzialną za umowy (telefon komórkowy).

> Następnie przejdź do sekcji 2.3: Sprawdzanie zawartości przesyłki

2.3 Sprawdzanie zawartości przesyłki

Jeśli otrzymałeś smartfon/tablet od swojego centrum kosztów lub osoby odpowiedzialnej za umowy (telefon komórkowy) albo poprzez zamówienie złożone w sklepie internetowym Digitalshop, zacznij od następujących kroków:

Czy wszystko jest na miejscu?

- Smartfon lub tablet
- Instrukcja obsługi, dokument przekazania, warunki użytkowania oraz narzędzie do wkładania karty SIM

Jeśli zamówiono:

- Akcesoria, takie jak kabel do ładowania, etui ochronne i power bank
- Pismo dotyczące karty SIM (wysłane przez Vodafone; zapytaj swojego doradcę ds. umów (komórkowych) tutaj)

2.4 Krótki przewodnik po konfiguracji smartfona/tabletu

Wraz ze smartfonem/tabletem otrzymasz drukowaną ulotkę.

Jeśli nie chcesz zapoznawać się z długimi instrukcjami konfiguracji, skorzystaj z ulotki:



> Jeśli nie masz jej pod ręką, możesz ją również znaleźć w Internecie pod adresem www.db.de/ae

> Zapisz skrócony link do wszystkich informacji dotyczących konfiguracji: db.de/mobile-setup

> Skróć do wszystkich informacji dotyczących resetowania/przywrócenia urządzenia: db.de/mobile-restore

3 Wymagania wstępne: Użytkownik bazy danych

Jeśli nie wiesz, kim jest użytkownik bazy danych, lub nie masz pewności, czy nim jesteś, przeczytaj tę sekcję.

3.1 Jesteś już członkiem grupy DB i użytkownikiem bazy danych

> Jeśli masz już konto użytkownika bazy danych, przejdź do rozdziału 4: Wstępna konfiguracja dla Samsung/HMD

3.2 Jesteś nowy w grupie DB, wymagane konto: użytkownik DB

Jeśli jesteś nowym członkiem Grupy DB, będziesz potrzebować konta użytkownika bazy danych, aby skonfigurować smartfon lub tablet. Konto użytkownika bazy danych zapewnia bezpłatny dostęp do wielu aplikacji grupy.

Czym jest konto użytkownika DB?

DB User to konto użytkownika dla wszystkich pracowników w ramach Grupy DB. Składa się z wybranego przez Ciebie hasła oraz automatycznie wygenerowanej nazwy logowania. Najpierw musisz mieć utworzone konto użytkownika DB (przez dział kadry).

Jak aktywować konto DB User?

Konto DB User aktywuje się jednorazowo, **wspólnie ze sponsorem**. Podczas tego procesu ustalasz hasło do konta DB User. Tutaj możesz zobaczyć, jak to działa i kto jest Twoim sponsorem:

> <https://db-planet.deutschebahn.com/pages/db-user/apps/content/konto-aktivierung>

Po zakończeniu aktywacji otrzymasz dokument PDF zawierający nazwę użytkownika DB.

Jak zmienić hasło do konta użytkownika DB?

> Jeśli zapomniałeś hasła, możesz je zmienić na stronie <https://self-service.service.deutschebahn.com/my.policy>

> Lub postępuj zgodnie z instrukcjami w rozdziale 10.1: Zapomniane lub zmiana hasła użytkownika DB

4 Wstępna konfiguracja dla Samsung/HMD

4.1 Wkładanie karty SIM

W górnej lub dolnej części smartfona/tabletu znajduje się mała przegródka.

- Otwórz tackę za pomocą narzędzia. Znajdziesz je w opakowaniu urządzenia
- Wyciągnij uchwyt karty i włóż kartę SIM
- Włóż uchwyt karty z powrotem do smartfona/tabletu



4.2 Kod PIN karty SIM

Podłącz smartfon/tablet do sieci za pomocą zasilacza.

- Naciśnij przycisk „Zasilanie”
- Po uruchomieniu urządzenia pojawi się prośba o podanie kodu PIN. Jest to kod PIN karty SIM, którą właśnie włożyłeś do urządzenia

Kod PIN można uzyskać w następujący sposób:

- Otwórz list od Vodafone dotyczący karty SIM
- Zdejmij folię. Pod spodem znajdziesz kod PIN i Super-PIN
- Wpisz kod PIN w polu wprowadzania danych na smartfonie/tablecie i potwierdź, klikając „OK”

4.3 Skonfiguruj blokadę ekranu

Następnie odblokuj urządzenie:

- Przesuń palcem po ekranie raz
- Zostaniesz poproszony o podanie „hasła”
- Wprowadź następujące hasło: **DB-Device2019**
- Naciśnij „OK”



- Możesz zmienić blokadę ekranu teraz lub później. Aby to zrobić, przejdź do sekcji 4.11 Zmiana blokady ekranu

4.4 Konfiguracja Wi-Fi

Aby skonfigurować Wi-Fi, wybierz jedną z następujących opcji:

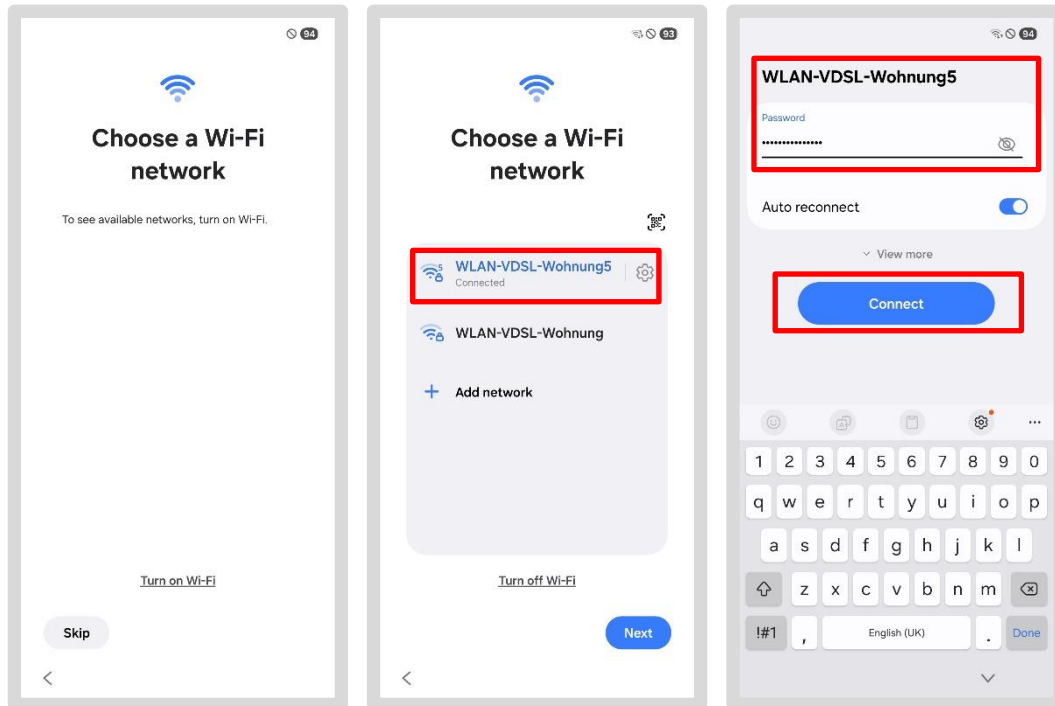
- Użyj danych komórkowych, pod warunkiem, że masz kartę SIM w smartfonie/tablecie (może to wiązać się z opłatami!)
- Skonfiguruj hotspot przy użyciu swojego smartfona/tabletu

lub

- Skorzystaj z hotspotu na smartfonie/tablecie kolegi z DB
- W przypadku smartfonów/tabletów Samsung: Skorzystaj z Wi-Fi dbs4mobile, jeśli zarezerwowałeś tę usługę (zobacz: <https://dbquestions.extranet.deutschebahn.com/question/27780>)
- Skorzystaj z własnej sieci Wi-Fi, jeśli pracujesz z domu

Aby wybrać inną sieć Wi-Fi, postępuj w następujący sposób:

- Dotknij sieci Wi-Fi, którą chcesz wybrać
- Wprowadź swoje dane logowania i dotknij „Połącz”
- Jeśli pojawi się drugi monit, dotknij „Kontynuuj”



Gdy tylko urządzenie połączy się z siecią Wi-Fi, rozpocznie się połączenie z siecią DB.

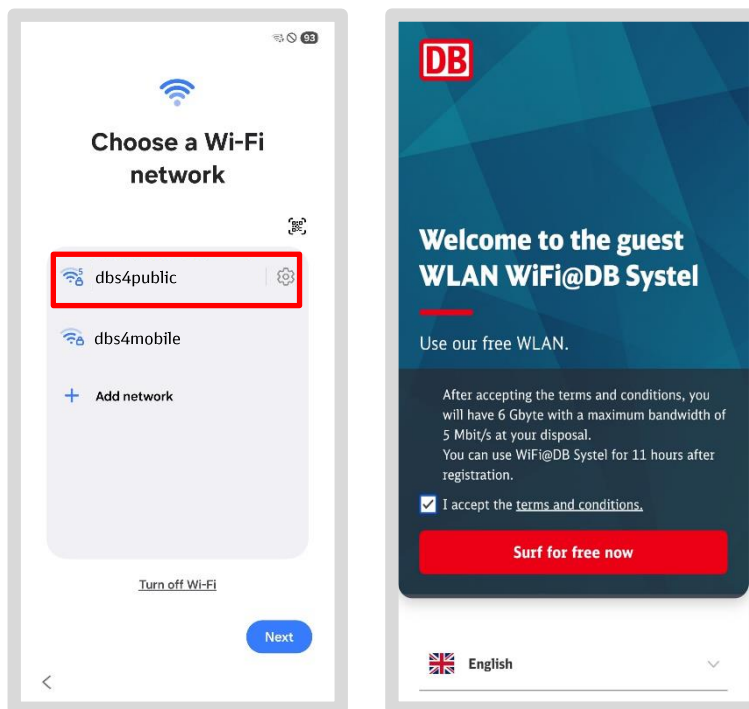
> Przejdź do [rozdziału 5: Treści służbowe i prywatne](#)

4.5 Konfiguracja Wi-Fi w budynkach DB

Ponieważ sieć Wi-Fi „dbs4public” nie zawsze działa zadowalająco w budynkach DB, zalecamy wykonanie jednej z czynności opisanych w [rozdziale 4.4 Konfiguracja Wi-Fi](#).

Jeśli znajdujesz się w **budynku DB** i chcesz skorzystać z sieci Wi-Fi „dbs4public”, postępuj w następujący sposób:

- Kliknij sieć Wi-Fi „dbs4public”
- Otworzy się okno dialogowe; zaakceptuj warunki
- Kliknij „Surfuj za darmo teraz”



Gdy tylko urządzenie połączy się z siecią Wi-Fi, rozpocznie się połączenie z siecią DB.

> Przejdź do [sekcji 4.6 Aktywacja urządzenia: utwórz tymczasową legitymację pracownika DB \(TAP\)](#)

4.6 Aktywacja urządzenia – Utwórz tymczasową legitymację pracownika DB (TAP)

Aby skonfigurować smartfon lub tablet w sieci DB, potrzebne będą:

- Ważna tymczasowa legitymacja pracownika DB (TAP) – db.de/tap
- nazwa użytkownika DB i hasło użytkownika DB
- *Aplikacja Intune*

Dla Twojej informacji:

DB User to konto użytkownika dla wszystkich pracowników Grupy DB. Składa się z wybranego przez Ciebie hasła oraz automatycznie wygenerowanej nazwy logowania.

- Hasło do konta DB User można zresetować na stronie db.de/passwort
- **Instrukcje dotyczące zmiany hasła użytkownika DB** znajdziesz w sekcji [Zmiana hasła użytkownika DB](#)
- Informacje o tym, **jak uzyskać dostęp do konta DB User**, można znaleźć w sekcji [Wymagania wstępne: DB User](#)
- **Nazwę użytkownika DB** można znaleźć w DeBi w sekcji db.de/debi

> **Uwaga:** Film instruktażowy można znaleźć na stronie db.de/mobile-videoanleitung

Istnieje kilka sposobów utworzenia tymczasowej legitymacji pracownika DB (TAP):

Opcja 1:

Masz **drugi smartfon/tablet** lub komputer BKU/Basic Workplace, który jest już zalogowany do sieci DB. W takim przypadku pozostań w bieżącym rozdziale i przejdź do następnej strony.

Opcja 2:

Kolega z tej samej firmy (np. DB Sales lub DB Long-Distance) może Ci pomóc, pod warunkiem, że posiada smartfon/tablet DB (lub iPhone/iPad) lub komputer BKU/Basic Workplace. Przejdź do:

> [Rozdział 4.7 Utwórz tymczasową legitymację pracownika DB dla współpracownika](#)

Ważne!

Po otrzymaniu **nowego smartfona/tabletu** nie można początkowo utworzyć tymczasowej legitymacji pracownika DB (TAP) przy użyciu tego urządzenia.

Jeśli nadal masz zainstalowaną aplikację Welcome:

- otwórz aplikację Welcome i kliknij „Pomoc”
- Następnie kliknij „Tymczasowa legitymacja pracownika DB (TAP)”, aby ją utworzyć

Jeśli nie masz zainstalowanej aplikacji Welcome:

- Wejdź na [stronę db.de/tap](https://db.de/tap) i wprowadź swoją nazwę użytkownika DB oraz hasło użytkownika DB
- Wybierz „Dla siebie” i naciśnij niebieski przycisk
- Teraz wybierz „DB Workplace Mobile”
- Wyświetli się tymczasowa legitymacja pracownika DB (TAP)
- Jest on **ważny przez 60 minut** i można go używać **na wielu smartfonach/tabletach**

Create a Temporary Access Pass (TAP)
This self-service allows you to create a temporary access pass (TAP) to set up a DB Workplace or Basic Workplace device.

The TAP can be created for:

- yourself
- an employee from the same company (see [EVI](#))

Register
Enter your DB user login details

DB User Anmeldenname
Max Mustermann

DB User Password

[How can I log in to other environments?](#)

Create a Temporary Access Pass (TAP) - Person selection

Choose for whom the TAP should be created:

For myself

For another DB employee

Create a Temporary Access Pass (TAP)
Select the product you want to set up.

DB Workplace Mobile
I want to set up a smartphone/tablet.

Basic Workplace Windows
I want to set up a notebook / PC.

DB Workplace Windows
I want to set up a notebook / PC.

Create a Temporary Access Pass (TAP)

y&r3%9=cg2u#

Enter the Temporary Access Pass (TAP) to activate your DB Workplace Mobile device, following the instructions. This is valid until **3:34 p.m.** and can be used **several times**.

Start a new session To the homepage

Uwaga!

Kod **TAP** można wprowadzić wyłącznie w **aplikacji Intune**, nawet jeśli zostaniesz o to poproszony w innej aplikacji DB lub na innym urządzeniu.

- Zapisz tymczasową legitymację pracownika DB na kartce papieru lub w notatniku
- Będzie on potrzebny później podczas konfiguracji i aktywacji w *aplikacji Intune*
- Teraz możesz aktywować swój smartfon/tablet w *aplikacji Intune*

> Przejdź bezpośrednio do [rozdziału 4.8: Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB](#)

Ważne!

Twój smartfon/tablet nie jest jeszcze podłączony do sieci DB!

Wprowadź **tymczasową legitymację pracownika DB** w *aplikacji Intune*.

Aby to zrobić, postępuj zgodnie z instrukcjami krok po kroku zawartymi w

> [Rozdział 4.8 Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB \(TAP\)](#)

4.7 Utwórz tymczasową legitymację pracownika DB dla współpracownika

Aby utworzyć TAP dla współpracownika, postępuj zgodnie z poniższymi instrukcjami:

Jeśli nadal masz zainstalowaną aplikację Welcome:

- Otwórz aplikację *Welcome* i kliknij „Pomoc”
- Następnie kliknij „Tymczasowa legitymacja pracownika DB (TAP)”, aby ją utworzyć

Jeśli nie masz zainstalowanej aplikacji Welcome:

- Wejdź na [stronę db.de/tap](https://db.de/tap) i wprowadź swoją nazwę użytkownika DB oraz hasło użytkownika DB
- Wprowadź swoją nazwę użytkownika DB i hasło użytkownika DB
- Wybierz opcję „Dla innego pracownika DB” i naciśnij niebieski przycisk

Create a Temporary Access Pass (TAP)

This self-service allows you to create a temporary access pass (TAP) to set up a DB Workplace or Basic Workplace device.

The TAP can be created for:

- yourself
- an employee from the same company (see [EVI](#))

Register

Enter your DB user login details

DB User Anmeldename
Max Mustermann

DB User Password

[How can I log in to other environments?](#)

Create a Temporary Access Pass (TAP) - Person selection

Choose for whom the TAP should be created:

For myself

For another DB employee

Max Mustermann

DB User: [blurred]

Name: [blurred]

E-mail: [blurred]

Department: [blurred]

Company: DB Systel GmbH

I confirm that I have established the employee's identity.

- Wybierz właściwą osobę, potwierdź jej tożsamość i naciśnij przycisk
- Przekaż kontrolę w Teams koledze podczas pracy zdalnej za pośrednictwem Teams lub
- Pozwól współpracownikowi korzystać z komputera
- Kolega wprowadza hasło użytkownika DB
- Następnie wyświetli się legitymacja pracownika DB; **jest ona ważna przez 60 minut i można ją używać na wielu smartfonach/tabletach**
- Odzyskaj kontrolę nad ekranem, jeśli korzystałeś z aplikacji Teams
- Zapisz tymczasową legitymację pracownika DB na kartce papieru lub w notatniku

Create a Temporary Access Passport (TAP) for Max Mustermann

The selected employee must personally enter their DB User access data here.

Register

DB User Anmeldename
Max Mustermann

DB User Password

Note for DB employees: Never share your DB user login details with others.

Create a Temporary Access Pass (TAP)

y&r 3%9=c g2u#

Enter the Temporary Access Pass (TAP) to activate your DB Workplace Mobile device, following the instructions. This is valid until **3:34 p.m.** and can be used **several times**.

Start a new session To the homepage

- Będzie to potrzebne później do skonfigurowania i aktywacji urządzenia w *aplikacji Intune*
- Współpracownik może teraz aktywować swój smartfon/tablet w *aplikacji Intune*

> Przejdź bezpośrednio do rozdziału 4.8: Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB

Ważne!


Twój smartfon/tablet nie jest jeszcze podłączony do sieci DB!
Wprowadź **tymczasową legitymację pracownika DB** w *aplikacji Intune*.

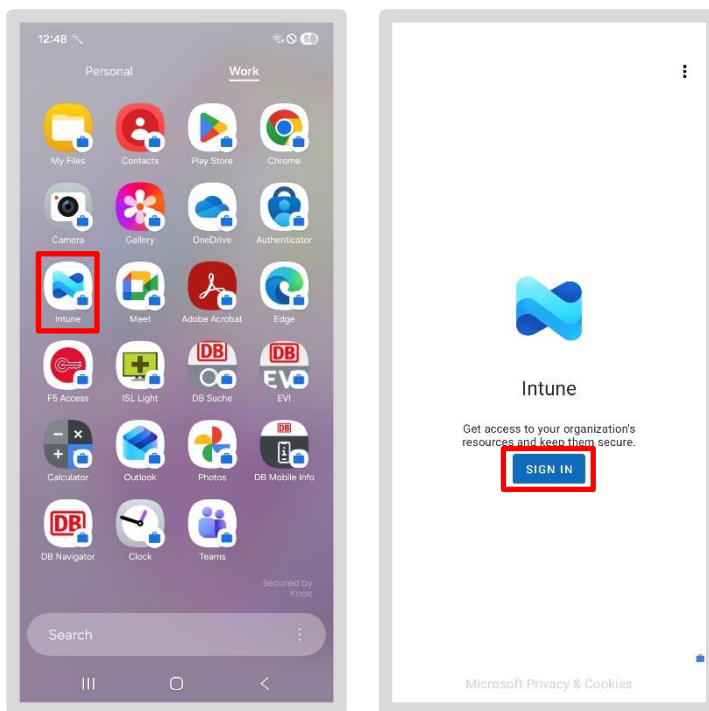
Aby to zrobić, postępuj zgodnie z instrukcjami krok po kroku zawartymi w > Rozdział 4.8 Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB (TAP)

4.8 Aktywacja urządzenia za pomocą tymczasowej legitymacji pracownika DB (TAP)

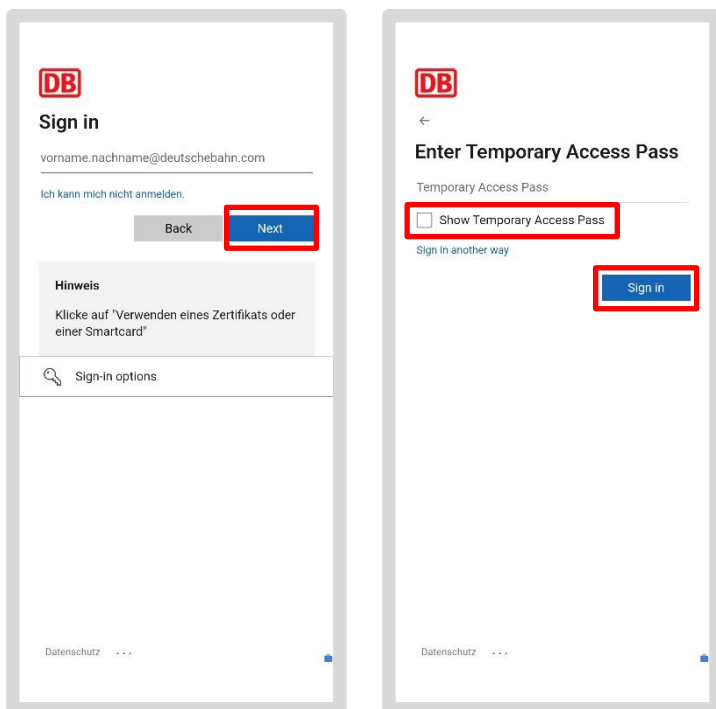
> **Uwaga:** Sprawdź, czy otrzymałeś tymczasową legitymację pracownika DB (TAP), zgodnie z opisem w rozdziale 4.6 Aktywacja urządzenia – Utwórz tymczasową legitymację pracownika DB (TAP)!

> **Uwaga:** Film instruktażowy można znaleźć na stronie db.de/mobile-videoanleitung

- Aplikacja *Welcome* nie jest już wymagana do aktywacji; w tym celu dostępna jest teraz aplikacja *Intune*
- Przejdź do sekcji „Praca”/„Biznes”, przesuwając palcem w górę od dołu
- Otwórz aplikację  *Intune*
- Następnie naciśnij przycisk „Zaloguj się”



- Wprowadź swój **adres e-mail użytkownika DB** (nie: użytkownik DB) i dotknij „Dalej”
- **Wskazówka:** Zaznacz pole obok opcji „*Pokaż tymczasową legitymację pracownika DB*”
- Wprowadź tymczasową legitymację pracownika DB i dotknij „Zaloguj się”



Ważne: Wprowadź tymczasową legitymację pracownika DB wyłącznie w aplikacji Intune!

Jeśli pojawi się komunikat o błędzie:

- Utwórz nowe tymczasowe hasło dostępu i powtórz proces logowania zgodnie z opisem w rozdziale 4.6 Aktywacja urządzenia – Utwórz tymczasową legitymację pracownika DB (TAP)

> Przejdź do rozdziału 4.9 Konfiguracja dostępu do wszystkich aplikacji i stron internetowych DB

Uwaga: Jeśli tymczasowa legitymacja pracownika DB (TAP) jest ważna (w ciągu 60 minut) i otworzysz np. aplikację Outlook, Teams lub IT ServiceDesk, zostaniesz poproszony o podanie tymczasowej legitymacji pracownika DB; wprowadź tutaj również tymczasową legitymację pracownika DB, którą zapisałeś.

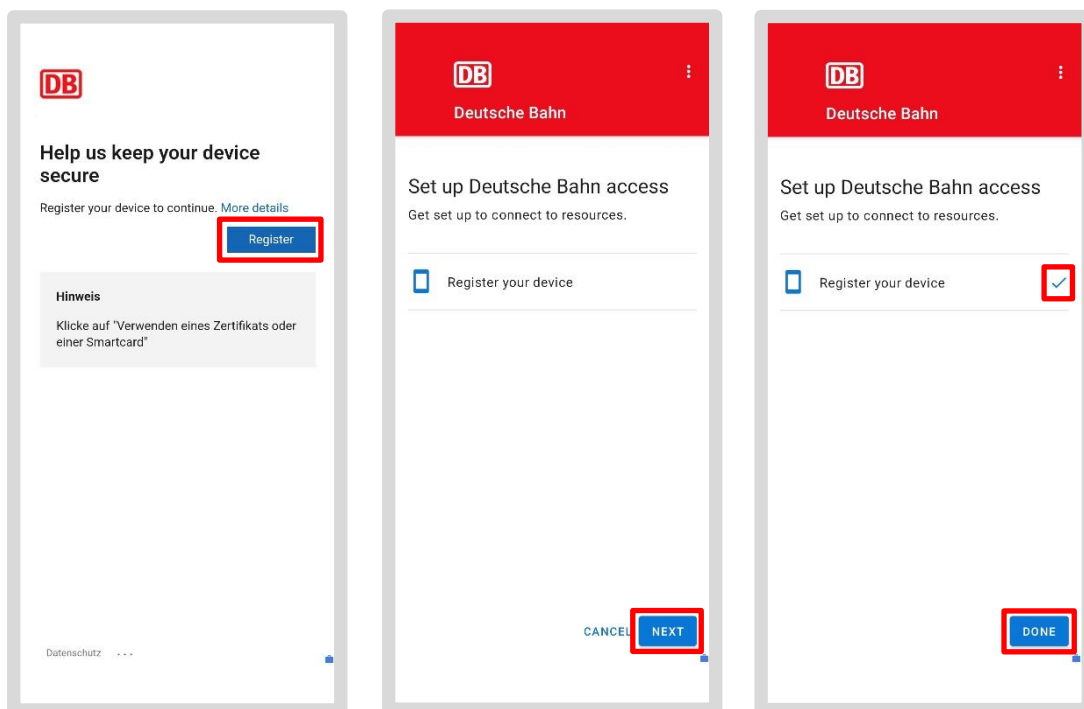
4.9 Konfiguracja dostępu do wszystkich aplikacji i stron internetowych DB

Trwa konfiguracja dostępu do sieci DB:

- Naciśnij „Zarejestruj”, a następnie „Dalej”
- Gdy obok opcji „Zarejestruj urządzenie” pojawi się znacznik wyboru, naciśnij przycisk „Gotowe”

Uwaga: Jeśli przycisk „Gotowe” nie pojawi się, aktywacja nie została zakończona

- Otwórz ponownie aplikację *Intune* i wykonaj krok po kroku czynności opisane w rozdziale 6, „Aktywacja urządzenia w DB”



> **Uwaga: Po rejestracji poczekaj od 5 minut do 24 godzin!**

Gdy wszystkie informacje i certyfikaty zostaną przeniesione na smartfon lub tablet, można korzystać z aplikacji, takich jak Outlook, Teams itp.

4.10 Aplikacje DB

Uwaga: Wydanie certyfikatów może potrwać **od 5 minut do 24 godzin**. Dopiero wtedy można korzystać z aplikacji, takich jak Outlook, Teams itp.

Po zakończeniu konfiguracji aplikacji DB, takie jak aplikacja Outlook lub aplikacja Teams, zostaną pobrane automatycznie.

Następnie zostaną pobrane aplikacje specyficzne dla Twojej firmy lub działalności.

Możesz pobrać kolejne aplikacje DB ze sklepu Google Play Store (aplikacja z ikoną walizki) w obszarze „Praca”.

Aplikacja Welcome nie jest już dostępna na smartfonie/tablecie DB; zamiast niej dostępna jest **aplikacja DB MOBIL**, która zawiera wszystkie informacje, przydatne linki i dane dotyczące smartfona/tabletu DB.

4.11 Zmiana blokady ekranu

Blokada ekranu to osobiste hasło lub osobista kombinacja cyfr, którą sam ustalasz, aby zapewnić bezpieczeństwo smartfonowi/tabletowi.

W następnym kroku zmień blokadę ekranu i ustaw nowe hasło lub nową 6-cyfrową kombinację. Zwróć również uwagę na informacje dotyczące prywatności i użytkowania.

Ponadto można skonfigurować tzw. „zabezpieczenie biometryczne”. Umożliwia to odblokowanie smartfona/tabletu za pomocą odcisku palca lub rozpoznawania twarzy.

Postępuj w następujący sposób:

- Przejdź do sekcji „Ustawienia”
- Naciśnij aplikację „Ustawienia” w sekcji „Osobiste”/„Prywatność”
- Lub przesuń palcem w dół raz od góry ekranu
- Otworzy się pasek z ikonami
- Naciśnij ikonę koła zębatego w prawym górnym rogu
- Kliknij „Ekran blokady” i wybierz „Typ ekranu blokady”
- Wprowadź aktualny kod blokady ekranu. Przy pierwszym użyciu będzie to hasło z kroku „Odblokuj” (**DB-Device2019**)



W przypadku tabletów:

- W poniższym oknie wybierz „Nie, dziękuję” i dotknij „Dalej”

Następnie kontynuuj:

- Wybierz „PIN” lub „Hasło”
- Wprowadź nowe hasło lub kod PIN. Pamiętaj, aby je zapamiętać!

Jeśli chcesz skonfigurować zabezpieczenia biometryczne:

- W sekcji „Dane biometryczne” wybierz „Odciski palców” lub „Twarz”
- Zeskanuj odcisk palca lub twarz
- Wprowadź aktualne hasło/kod PIN urządzenia
- Urządzenie zeskanuje teraz Twoją twarz (Uwaga: jeśli nosisz okulary, musisz je zdjąć podczas skanowania)
- Po skonfigurowaniu funkcji rozpoznawania twarzy pojawi się powiadomienie
- Potwierdź komunikat „Szybkie rozpoznawanie twarzy”, dotykając „OK”

4.12 Take-Off: „Zaloguj się na smartfonie/tablecie

Aby skonfigurować smartfon/tablet DB po raz pierwszy, potrzebne będą:

Karta SIM i kod PIN karty SIM

- Karta SIM jest potrzebna do wykonywania połączeń za pomocą smartfona/tabletu. Kartę SIM i kod PIN znajdziesz w liście od Vodafone, który został wysłany do Ciebie wcześniej
- Musisz wprowadzić kod PIN karty SIM przy każdym włączeniu urządzenia. Jeśli go zapomniałeś, zajrzyj [tutaj](#)

Hasło do blokady ekranu

- Początkowe hasło blokady ekranu to **DB-Device2019**
- Blokada ekranu to osobiste hasło lub osobista kombinacja cyfr – chroni ona smartfon/tablet przed nieautoryzowanym dostępem
- Następnie wybierz nowy kod PIN lub hasło, którego będziesz używać do odblokowywania smartfona/tabletu w przyszłości, i upewnij się, że je zapamiętasz

Nazwa użytkownika DB i hasło użytkownika DB

- Będziesz potrzebować nazwy użytkownika DB i hasła użytkownika DB, aby zalogować się do wielu aplikacji i stron internetowych DB
- Nazwa użytkownika DB składa się z imienia i nazwiska
- Hasło użytkownika DB ustalasz samodzielnie podczas aktywacji
- Jeśli zapomniałeś hasła, zmień je [na stronie https://self-service.service.deutschebahn.com/my.policcy](https://self-service.service.deutschebahn.com/my.policcy)

Uwaga: Niektóre narzędzia, takie jak ASES, mają własne hasła. Można je zapisać w aplikacji „Keepass2Android” (dotyczy to wyłącznie smartfonów/tabletów z systemem operacyjnym Android).

- Adres e-mail użytkownika DB i tymczasowa legitymacja pracownika DB do aktywacji
- Tymczasowa legitymacja pracownika DB (ważna przez ograniczony czas) można uzyskać za pośrednictwem aplikacji IT ServiceDesk
- Użyj go, aby zalogować się do *aplikacji Intune* i aktywować swój smartfon/tablet

Podsumowując:

Konfiguracja smartfona/tabletu DB – wykonaj następujące czynności:

- Włóż kartę SIM
- Włącz smartfon/tablet
- Uzyskaj tymczasową legitymację pracownika DB za pośrednictwem aplikacji IT ServiceDesk. Możesz to zrobić za pomocą drugiego smartfona/tabletu DB, komputera BKU/Basic Workplace lub za pośrednictwem kolegi
- Otwórz *aplikację Intune* i wprowadź tymczasową legitymację pracownika DB (TAP)

Wraz ze smartfonem/tabletem otrzymasz drukowaną ulotkę.

Pomoże Ci to w początkowej konfiguracji!

> Jeśli nie masz go pod ręką, możesz go również znaleźć online pod adresem db.de/mobile-setup

4.13 Wskazówki dotyczące codziennego włączania urządzenia

Od teraz przy włączaniu i wyłączaniu smartfona/tabletu należy zawsze wykonać następujące czynności:

- Odblokuj kartę SIM za pomocą kodu PIN podanego w piśmie od Vodafone
- Odblokuj smartfon/tablet za pomocą osobistego hasła/kodu PIN
- Lub urządzenie rozpoznaje użytkownika na podstawie odcisku palca lub twarzy

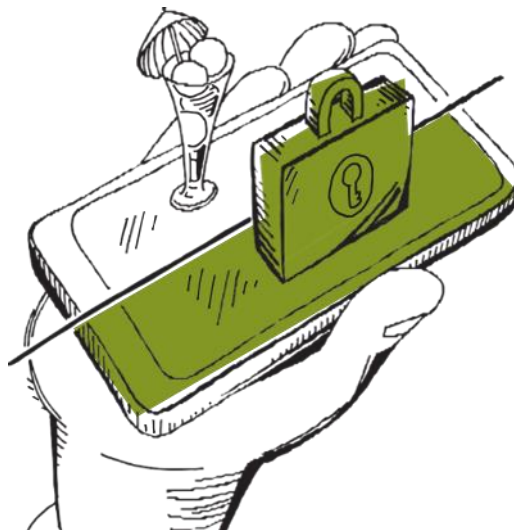
Jeśli urządzenie jest już włączone, wystarczy je odblokować za pomocą odcisku palca lub rozpoznawania twarzy.

5 Treści służbowe i prywatne

Na smartfonie/tablecie DB zainstalowana jest wersja Enterprise; można to rozpoznać po tym, że treści osobiste i służbowe są przechowywane oddzielnie:

- W urządzeniach Samsung/HMD treści i aplikacje związane z pracą są przechowywane w oddzielnej sekcji „Praca/Biznes”. Aplikacje służbowe można rozpoznać po ikonie teczki z kluczem oraz po szarej ikonie teczki w prawym górnym rogu obok ikony baterii.

W tym przewodniku zebraliśmy kilka wskazówek dotyczących korzystania z aplikacji, aby zapewnić, że dane służbowe i prywatne nie zostaną pomieszane. Zawsze przestrzegaj tej zasady:



Używaj aplikacji służbowych wyłącznie do zadań związanych z pracą!

5.1 Rozróżnienie między użyciem służbowym a prywatnym

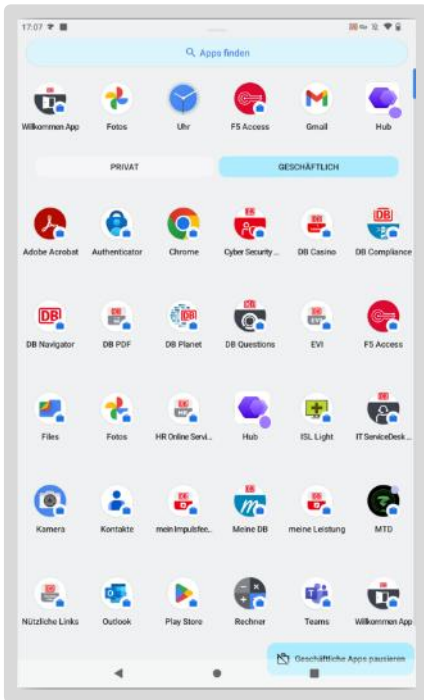
Użycie związane z pracą ma miejsce, gdy

- Rozpoczynasz swoją zmianę za pomocą aplikacji
- Lub otwierasz aktualny grafik dyżurów

Użycie prywatne obejmuje na przykład:

- Oglądanie Netflix
- Słuchanie Spotify
- Tworzenie konta Google

Uwaga: nie zawsze można jednoznacznie odróżnić użytkowanie służbowe od prywatnego. Dlatego należy zawsze dokładnie rozważyć, do czego używasz smartfona/tabletu.



Stanowisko firmy Nokia/HMD



Zobacz Samsung

Jak przejść do sekcji „Praca/Biznes”:

- Przesuń palcem w górę na ekranie głównym
- Naciśnij „Praca” lub „Biznes” w prawym dolnym rogu
- Zobaczysz teraz wszystkie swoje aplikacje służbowe

Jedyny wyjątek: aplikacja Telefon może służyć zarówno do połączeń służbowych, jak i prywatnych. Aby wykonać połączenie służbowe, dotknij aplikacji „Kontakty” służbowe, wybierz kontakt służbowy i dotknij ikony telefonu.

5.2 Pobierz aplikacje DB

Pobierz aplikacje służbowe z ikoną DB za pośrednictwem **sklepu DB Google Play** w sekcji „Praca” lub „Biznes”.

W razie potrzeby można zainstalować aplikacje do użytku prywatnego. W tym celu należy użyć **swojego prywatnego konta Google** lub utworzyć nowe, przestrzegając warunków użytkownika urządzenia.

5.3 Zarządzanie elementami na ekranie głównym

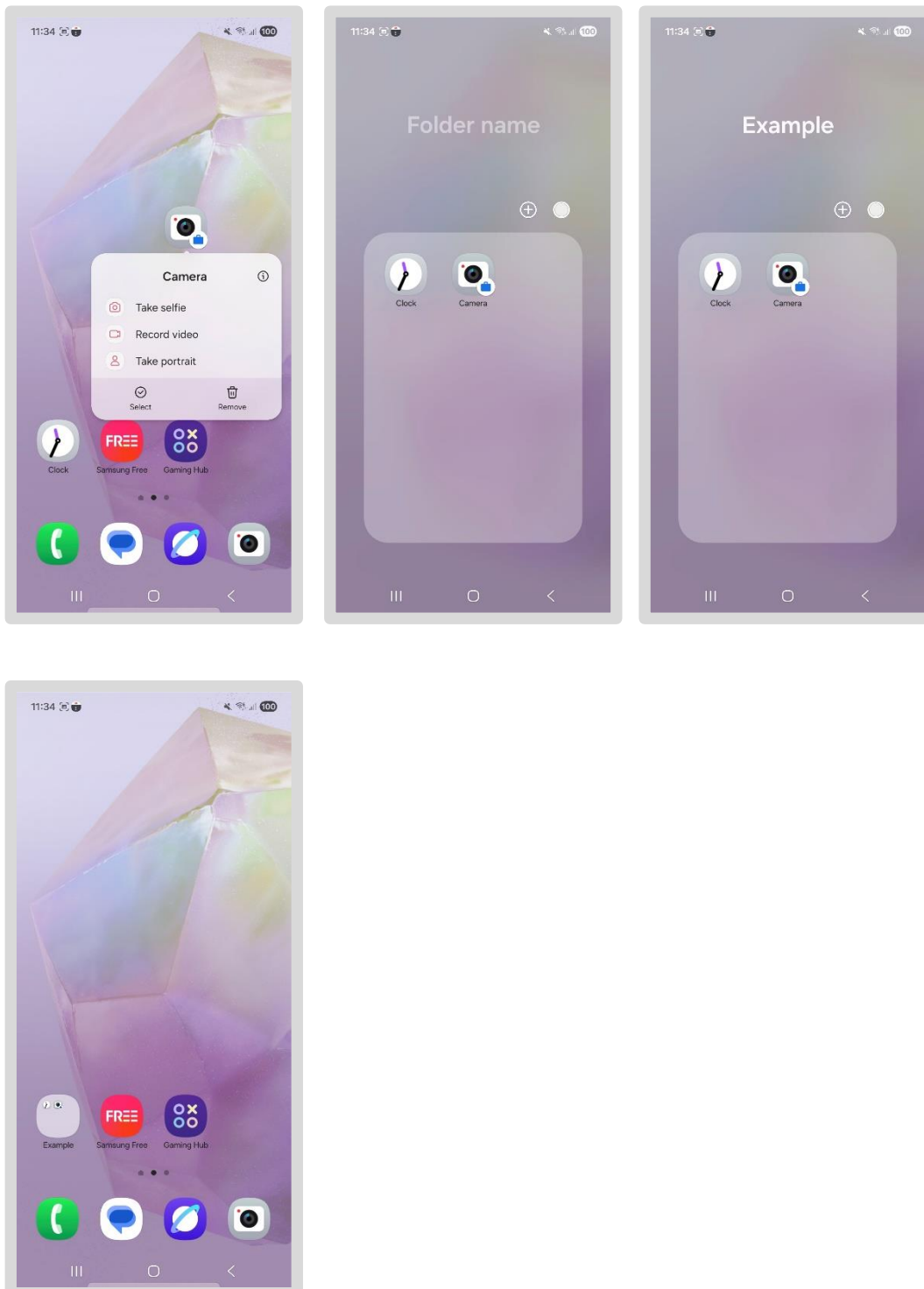
Możesz przeciągnąć aplikacje DB, z których korzystasz na co dzień, takie jak aplikacja aparatu służbowego, na ekran główny. Oto jak to zrobić:

- Naciśnij i przytrzymaj aplikację
- Nad aplikacją otworzy się małe okienko
- Naciśnij „Dodaj do ekranu głównego”
- Przeciągnij aplikację w lewo, aż pojawi się na wybranym ekranie głównym (Uwaga: urządzenie zazwyczaj ma kilka ekranów głównych).
- Puść aplikację; znajduje się ona teraz na wybranym ekranie głównym



Uwagi dotyczące grupowania

- Naciśnij i przytrzymaj aplikację
- Przeciągnij aplikację na inną aplikację, a następnie ją zwolnij
- Zostanie utworzona grupa lub folder
- Wpisz nazwę folderu lub grupy
- Jeśli chcesz dodać więcej aplikacji, przeciągnij je do grupy



5.4 Take-Off: Oddzielanie aplikacji osobistych od służbowych + grupowanie aplikacji

Twój smartfon/tablet jest tzw. urządzeniem służbowym. Aplikacje do pracy na urządzeniach Samsung/HMD znajdziesz w obszarze roboczym „Praca/Biznes”.

Private Apps



u.a. Play Store, Galerie

Dienstliche Apps



Używaj aplikacji służbowych wyłącznie do zadań związanych z pracą! Niektóre aplikacje są dostępne zarówno do użytku służbowego, jak i osobistego. Zdecyduj świadomie, które z nich chcesz wykorzystać do swoich konkretnych potrzeb.

Aplikacje DB, z których korzystasz na co dzień, możesz przeciągnąć na ekran główny. Możesz również grupować aplikacje, co zapewni Ci lepszy przegląd aplikacji DB.

6 Dalsze ustawienia

W następnym kroku pokażemy, jak dostosować smartfon/tablet do własnych potrzeb, aby jak najlepiej wspierał Cię w codziennej pracy.

6.1 System operacyjny

System operacyjny stanowi podstawę smartfona/tabletu. Jest to interfejs użytkownika, na którym instalowane są aplikacje i oprogramowanie.

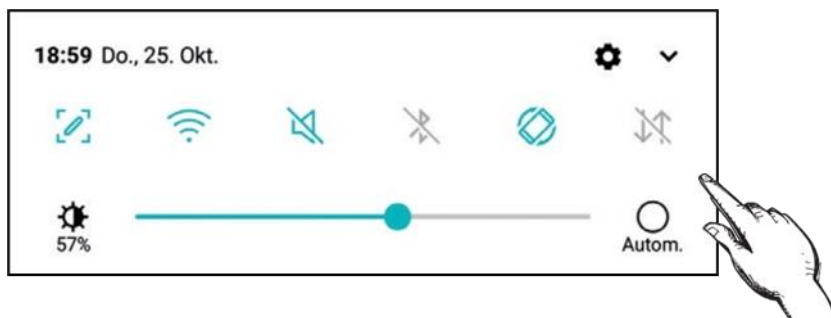
Urządzenie Samsung/HMD działa pod kontrolą systemu operacyjnego Android. Tutaj można sprawdzić, jaką wersję systemu operacyjnego posiada smartfon/tablet:

- Otwórz „Ustawienia”
- Przewiń do „Informacje o telefonie” lub „O telefonie”
- Naciśnij „Informacje o oprogramowaniu”. Wyświetli się aktualnie zainstalowana wersja Androida

6.2 Szybki dostęp/Centrum sterowania

Chcesz dostosować jasność, wyłączyć Wi-Fi lub otworzyć ustawienia smartfona/tabletu? Znajdziesz tę funkcję w menu „Szybki dostęp”:

- Przesuń palcem raz w dół od górnej krawędzi ekranu
- Otworzy się pasek z ikonami – to jest Szybki dostęp



Tutaj możesz włączać i wyłączać funkcje smartfona/tabletu, dotykając ich, na przykład:



WLAN



Mobile Daten



Ton

Regulacja jasności ekranu:

- Dotknij paska w panelu szybkiego dostępu i przesunij suwak do żądanej jasności
- Chcesz, aby jasność ekranu dostosowywała się automatycznie? Zaznacz pole „Auto” lub dotknij małej ikony słońca z literą „A” obok



W sekcji Szybki dostęp znajduje się jeszcze więcej funkcji. Aby je wyświetlić, ponownie przesunij palcem w dół od góry ekranu. Pojawią się kolejne ikony, takie jak latarka.



Aplikacja latarki jest również ukryta w tym miejscu



Więcej ustawień znajdziesz w sekcji „Ustawienia” z ikoną koła zębatego. Możesz ją znaleźć, przesuwając palcem w dół od góry ekranu.

6.3 Take-Off: Zarządzaj aplikacjami na ekranie głównym

6.3.1 Utwórz folder (grupę)

- Dotknij aplikacji lub skrótu
- Naciśnij i przytrzymaj
- Przeciągnij aplikację lub skrót na inną. Następnie zwolnij.
- Jeśli chcesz dodać więcej aplikacji do folderu, przeciągnij je na grupę

6.3.2 Zmień nazwę folderu (grupy)

- Dotknij grupy, której nazwę chcesz zmienić
- Następnie dotknij sugerowanej nazwy folderu
- Możesz również dotknąć sugerowanej nazwy u góry klawiatury lub wpisać własną nazwę

6.3.3 Przenoszenie aplikacji/folderów

Na smartfonie/tablecie możesz przenosić aplikacje i foldery w obrębie jednego ekranu lub z jednego ekranu na drugi:

- Naciśnij i przytrzymaj aplikację
- Następnie przeciągnij aplikację w wybrane miejsce i zwolnij

6.3.4 Przenoszenie aplikacji na ekran główny

- Naciśnij i przytrzymaj aplikację
- Przeciągnij aplikację bezpośrednio z sekcji „Praca/Biznes” na ekran główny

6.3.5 Tablet Samsung/HMD:

- Wszystkie aplikacje są wyświetlane w jednym widoku; nie można przeciągać aplikacji bezpośrednio z folderu
- Aby to zrobić, przesun palcem raz przez środek ekranu, a następnie w lewo
- Zobaczysz wtedy wszystkie swoje aplikacje służbowe
- Stamtąd możesz je przenieść w dowolne miejsce

6.4 Połącz się z Internetem

6.4.1 Wi-Fi DB

- Połącz się z siecią DB Wi-Fi (dbs4mobile) w lokalizacjach DB
- Pozwala to zaoszczędzić pakiet danych komórkowych, zapewniając jednocześnie bezpieczne połączenie sieciowe
- Wybierz odpowiednią sieć Wi-Fi DB
- Następnie włącz Wi-Fi w menu szybkich ustawień na smartfonie/tablecie
- Wprowadź dane logowania użytkownika DB; następnym razem urządzenie połączy się automatycznie



Uwaga: Aby korzystać z DB Wi-Fi, zamów usługę „Punkt dostępu bezprzewodowego DB Wi-Fi” w Sklepie Cyfrowym

6.4.2 Publiczne Wi-Fi

Bezpieczeństwo danych na smartfonie lub tablecie jest szczególnie ważne wszędzie tam, gdzie dostępne jest publiczne Wi-Fi.

- Loguj się wyłącznie przez DB Wi-Fi lub prywatną sieć Wi-Fi w domu
- Unikaj korzystania z niezabezpieczonych sieci Wi-Fi innych dostawców
- Ponadto, wybierając sieć, upewnij się, że korzystasz z właściwego Wi-Fi

Zawsze przestrzegaj ogólnych wytycznych DB dotyczących bezpieczeństwa



6.4.3 Informacje o transmisji danych – limit danych

Jeśli w pobliżu nie ma sieci Wi-Fi DB, korzystaj z internetu za pomocą transmisji danych. W zależności od umowy Deutsche Bahn AG zapewnia limit danych, który umożliwia bezpłatne korzystanie z internetu.

- Gdy w bieżącym miesiącu wykorzystasz 80% tego limitu, otrzymasz wiadomość SMS
- Zostaniesz zapytany, czy chcesz doładować pakiet o dodatkowe dane
- Pamiętaj, że wiąże się to z kosztami dodatkowymi dla DB



6.4.4 Twoja umowa z Vodafone – Elfe (elektroniczny rachunek telekomunikacyjny)

Raz w miesiącu otrzymasz zestawienie dotyczące umowy z Vodafone na smartfon/tablet. Zostanie ono wysłane do Ciebie pocztą elektroniczną od nadawcy ELFE@deutschebahn.com. Aby otworzyć zestawienie, potrzebne będzie osobne hasło.

Otrzymasz je jednorazowo pocztą elektroniczną. Zachowaj hasło w bezpiecznym miejscu.



Ważne: Nie musisz nic płacić; wyciąg służy wyłącznie do celów dokumentacyjnych.

6.4.5 Wyłącz ostrzeżenie o wykorzystaniu danych

System operacyjny Android automatycznie wysyła ostrzeżenie, gdy tylko wykorzystasz 2 GB danych w ciągu miesiąca. Pomaga to śledzić zużycie danych.

Jednocześnie wszyscy użytkownicy Vodafone w Niemczech mają 6 GB danych podstawowych oraz automatyczny pakiet dodatkowy 2 GB (= łącznie 8 GB danych).

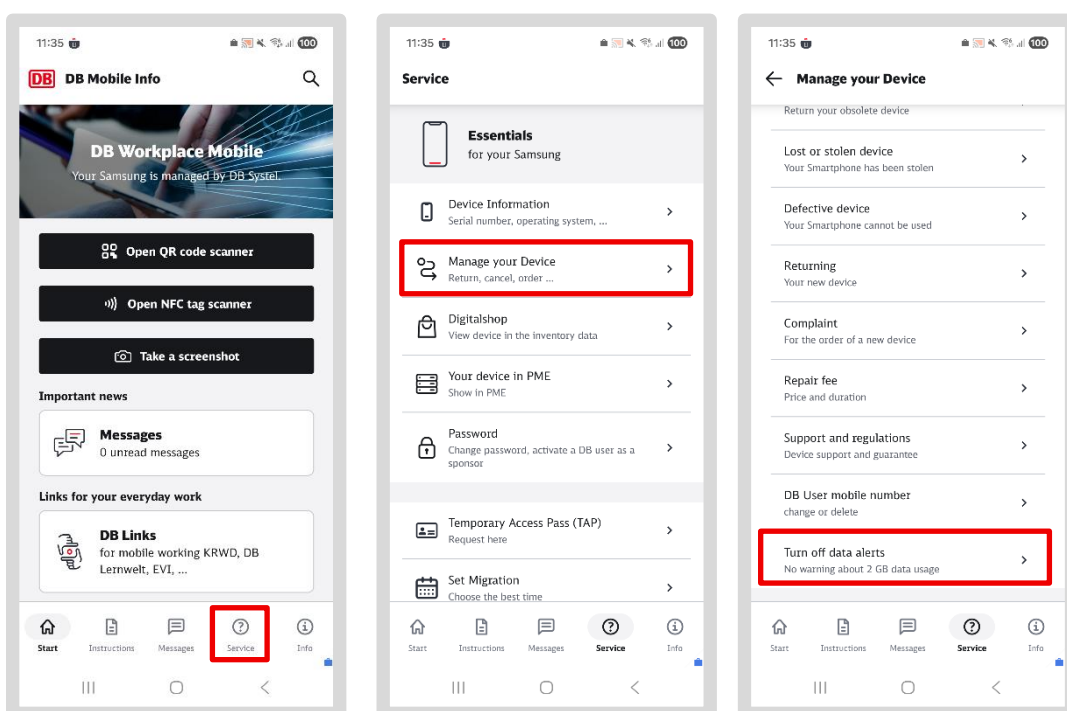
Jeśli więc nie chcesz otrzymywać ostrzeżenia po wykorzystaniu zaledwie 2 GB danych, możesz wyłączyć ostrzeżenie o wykorzystaniu danych w kilku prostych krokach. Możesz też zwiększyć domyślny limit.

Dobra wiadomość: nie musisz martwić się o nieoczekiwane koszty! Vodafone automatycznie powiadomi Cię SMS-em, gdy tylko wykorzystasz 80% swojego limitu danych (tj. 80% z 6 GB lub 8 GB) – niezależnie od tego, jakiego telefonu komórkowego używasz.

Jak wyłączyć ostrzeżenie o wykorzystaniu danych:

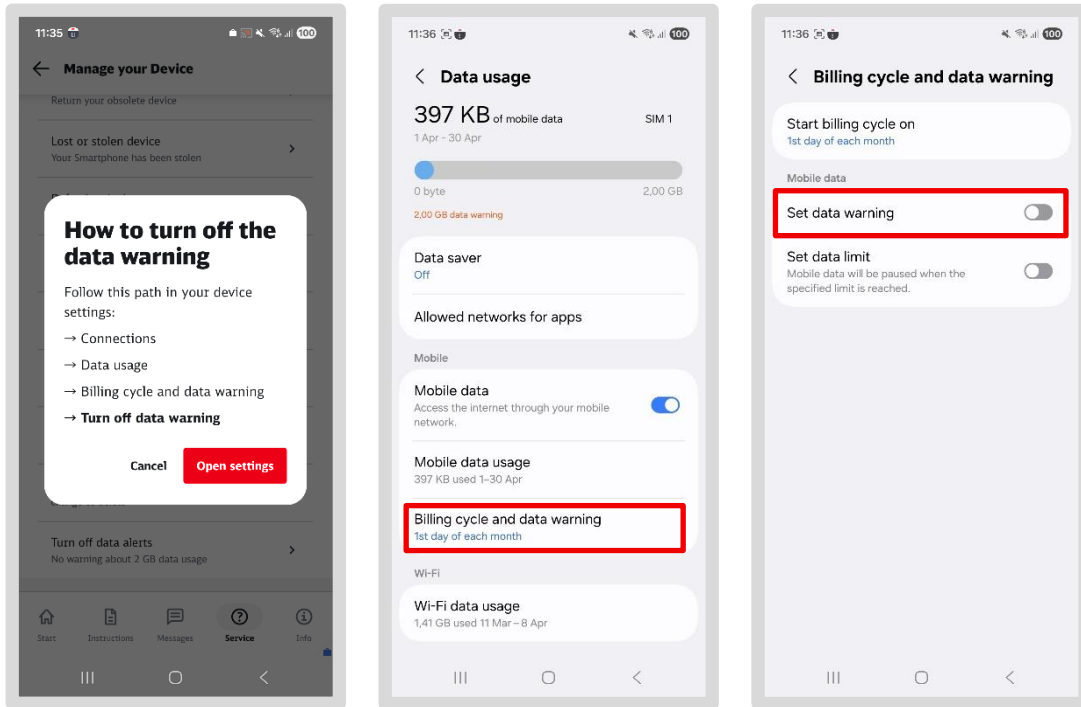
W przypadku smartfonów/tabletów Samsung wykonaj następujące czynności:

- Otwórz aplikację *DB MOBIL info*
- Naciśnij zakładkę „Usługi” → Następnie naciśnij „Wszystko o Twoim urządzeniu” → , a potem „Wyłącz ostrzeżenie o danych”



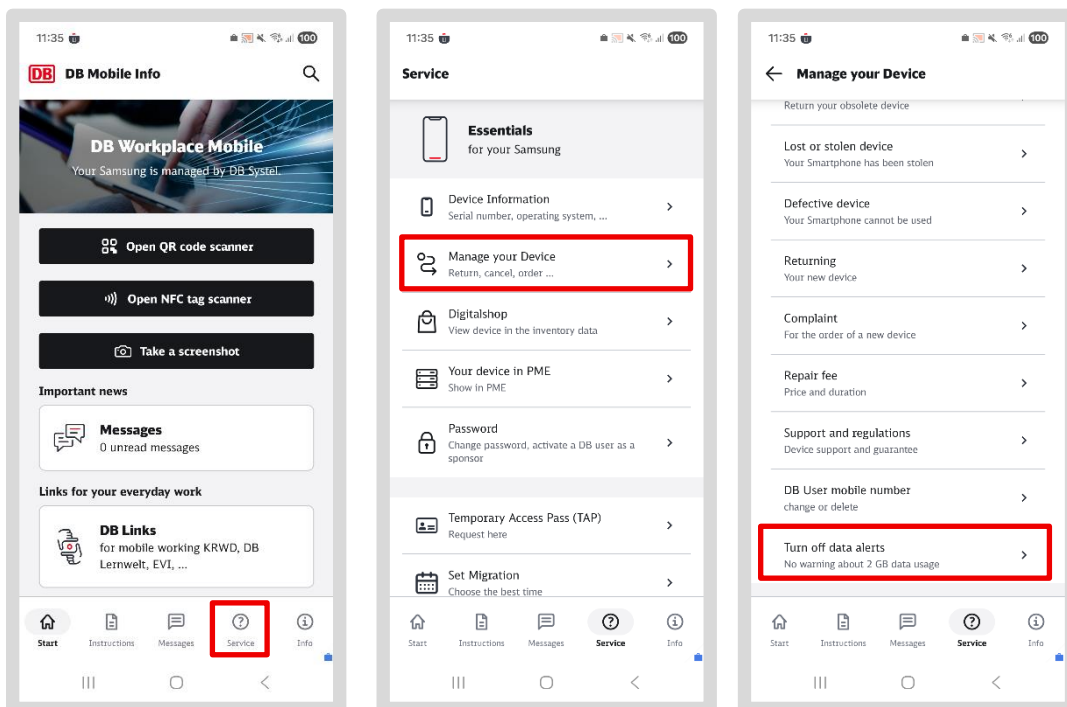
W ustawieniach systemowych otworzy się ekran „Połączenia”

- →Kliknij „Zużycie danych”, następnie „Cykl rozliczeniowy i ostrzeżenie o danych”, a w sekcji „Ustaw ostrzeżenie o danych” przesunąć palcem po ekranie w lewo



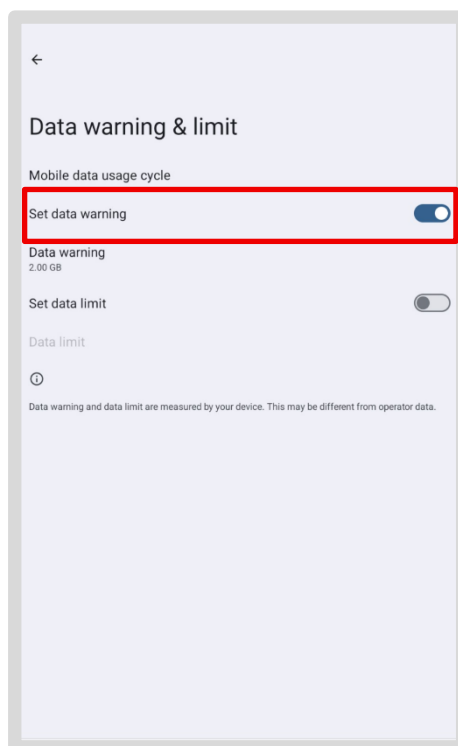
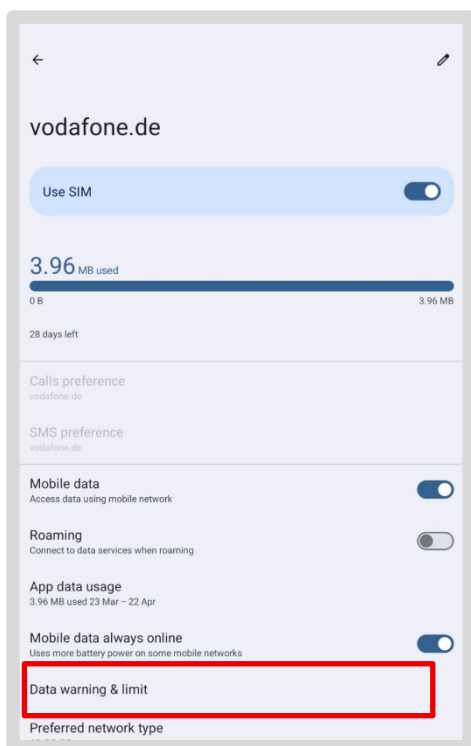
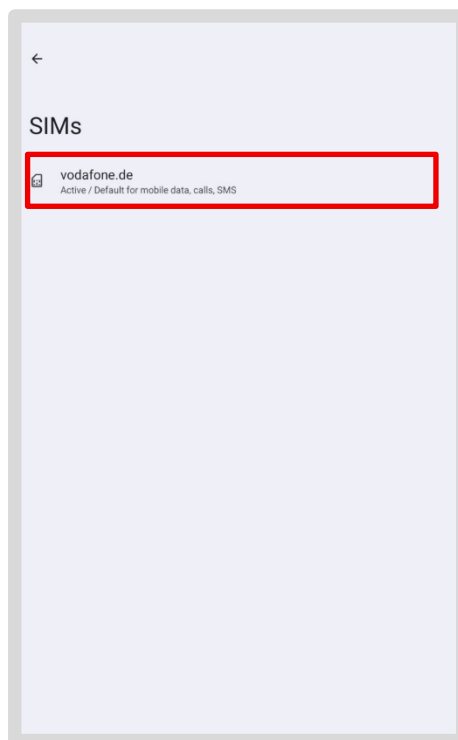
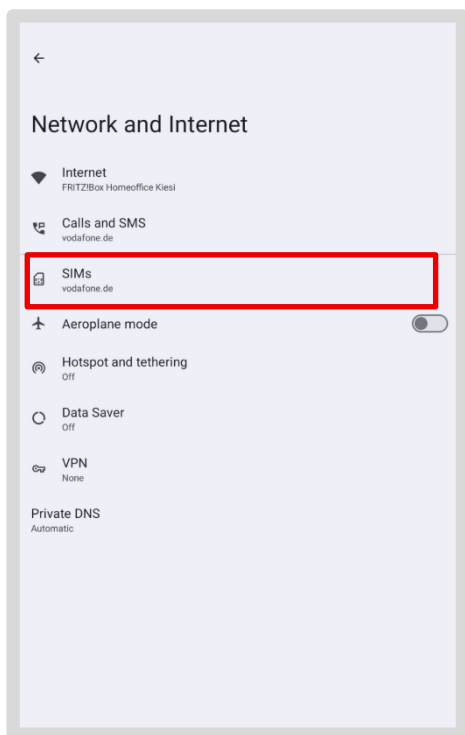
W przypadku smartfonów i tabletów Nokia/HMD wykonaj następujące czynności:

- Otwórz aplikację **DB MOBIL**
- Naciśnij zakładkę „Usługi” → Następnie naciśnij „Wszystko o Twoim urządzeniu” → , a potem „Wyłącz ostrzeżenie o danych”



W ustawieniach systemowych otworzy się ekran „Sieć i Internet”

- Naciśnij „Karty SIM” -> Naciśnij aktywną kartę SIM, w tym przypadku „vodafone.de” -> Naciśnij „Ostrzeżenie o danych i limit” i przesunij ekran w lewo w sekcji „Ustaw ostrzeżenie o danych”



6.4.6 Tryb offline (tryb samolotowy)

W menu szybkiego dostępu na smartfonie/tablecie możesz włączyć tryb offline lub tryb samolotowy. Pamiętaj jednak, że spowoduje to wyłączenie wszystkich funkcji komunikacyjnych. Oznacza to, że nie będą przeprowadzane żadne aktualizacje i nie będziesz otrzymywać żadnych wiadomości DB.



Dlatego dobrze się zastanów, kiedy włączasz tryb samolotowy.

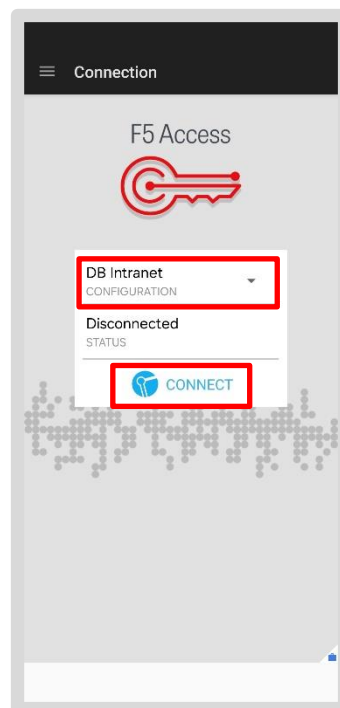
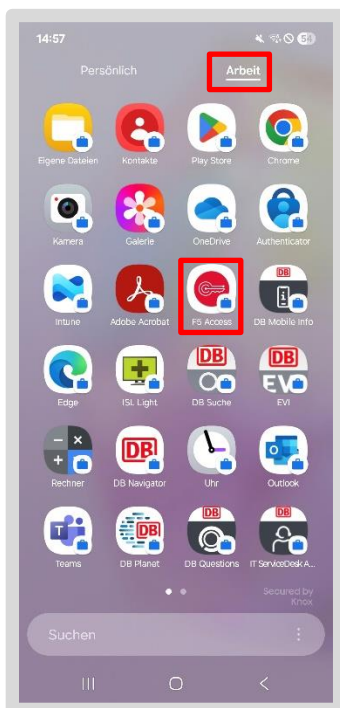
6.5 F5 Access – nawiąż połączenie VPN

VPN to skrót od **Virtual Private Network (wirtualna sieć prywatna)** i odnosi się do połączenia internetowego, którego nie mogą przeglądać nieuprawnione osoby trzecie. W Deutsche Bahn AG używamy „F5 Access” do nawiązania połączenia VPN. Daje to bezpieczny dostęp do sieci firmowej Deutsche Bahn AG. Co więcej, niektóre aplikacje można używać tylko z połączeniem VPN, np. portal DB Personal, ASES i E-Time.

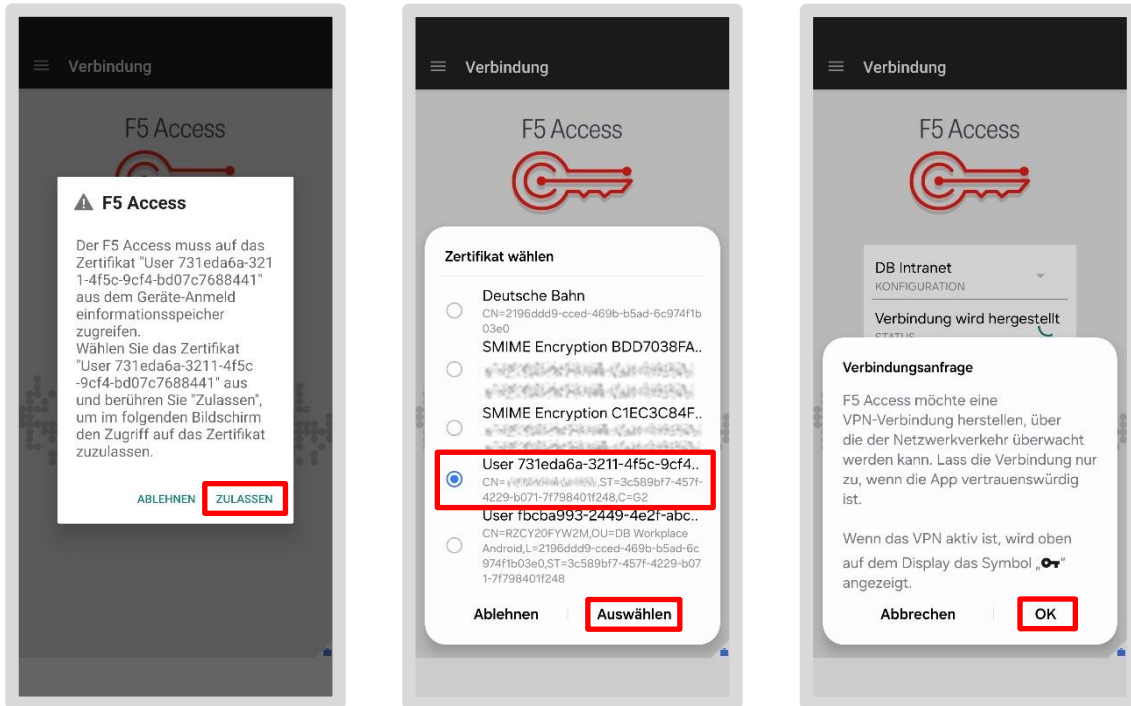


6.5.1 Skonfiguruj połączenie VPN

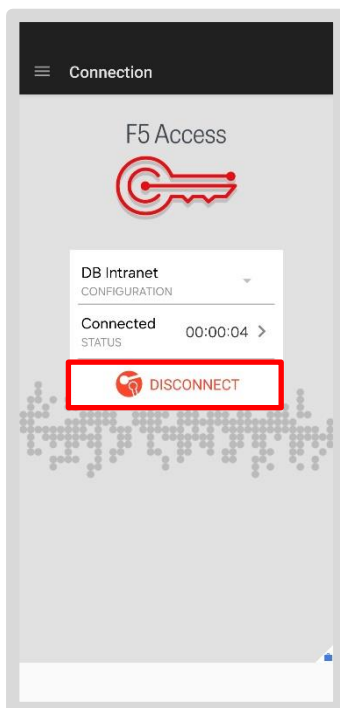
- Otwórz aplikację „F5 Access” w sekcji „Praca/Biznes”
- W razie potrzeby zaakceptuj warunki i zezwól na powiadomienia
- W sekcji „Konfiguracja” wybierz „DB Intranet”, a następnie „Połącz”
- Następnie zezwól na wykonywanie i zarządzanie połączeniami – wybierz „Zezwól”



- Następnie wybierz opcję „Zezwól” dla certyfikatu F5
- Wybierz certyfikat kończący się na C=G2
- Następnie dotknij „Wybierz”
- Następnie potwierdź żądanie połączenia, dotykając „OK”



- Aby się rozłączyć, dotknij „Rozłącz”



Uwaga: Stałe połączenie VPN powoduje duże zużycie baterii. Dlatego włączaj je tylko wtedy, gdy naprawdę tego potrzebujesz.

6.6 Take-Off: Certyfikaty i połączenie VPN

Dlaczego potrzebuję certyfikatu na moim smartfonie/tablecie?

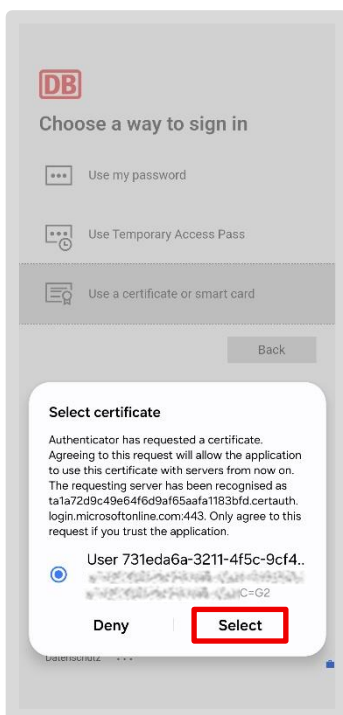
Aby uzyskać dostęp do niektórych aplikacji i stron internetowych DB na służbowym smartfonie/tablecie, musisz się zidentyfikować. Odbywa się to za pomocą tzw. certyfikatu. Certyfikat informuje aplikację lub stronę internetową, że jesteś uprawniony.

Jak uzyskać certyfikat?

Certyfikaty są automatycznie zapisywane na Twoim urządzeniu. Kiedy otwierasz aplikację po raz pierwszy, musisz raz wybrać certyfikat, a następnie zostaniesz zalogowany.

Na przykład w programie Outlook wygląda to tak:

Certyfikat zawsze zawiera imię i nazwisko użytkownika



Czym jest aplikacja F5 Access?

Aplikacja F5 Access jest automatycznie instalowana na smartfonie/tablecie. Ikona aplikacji wygląda tak:



Na urządzeniach Samsung/HMD znajdziesz ją w sekcji „Praca/Biznes”

Aplikacja F5 Access nawiązuje bezpieczne połączenie VPN między smartfonem/tabletem a intranetem DB. Wynika to z faktu, że niektóre aplikacje mobilne i strony internetowe wymagają takiego dostępu, aby się połączyć.

6.7 Wydłuż żywotność baterii

- Aktualizacje można zainstalować na smartfonie/tablecie tylko wtedy, gdy poziom naładowania baterii wynosi ponad 20%
- Jeśli aktualizacje nie zostaną zainstalowane, może to ostatecznie spowodować, że nie będziesz mógł korzystać ze smartfona/tabletu
- Dlatego zawsze upewnij się, że bateria jest wystarczająco naładowana!

Jak oszczędzać baterię:

- Wyłącz funkcje, które nie są potrzebne przez cały czas, np. Bluetooth, VPN (F5) i GPS
- Nie ładuj urządzenia przez całą noc
- Nie wystawiaj go na działanie ekstremalnych temperatur, zarówno zbyt niskich, jak i zbyt wysokich

6.8 Wyłącz identyfikator reklamowy

Domyślnie Google tworzy tzw. identyfikator reklamowy dla każdego smartfona/tabletu.

Google wykorzystuje identyfikator reklamowy do tworzenia profilu opartego na Twoim zachowaniu w sieci i preferencjach. Dzięki temu na Twoim smartfonie/tablecie mogą być wyświetlane spersonalizowane reklamy.

Urząd Ochrony Danych zaleca wyłączenie tego identyfikatora reklamowego. Jest to jedyny sposób, aby zapobiec utworzeniu profilu.

Aby to zrobić, wykonaj następujące czynności:

- Otwórz ustawienia na smartfonie/tablecie
- Naciśnij Google, a następnie Praca/Biznes
- Wybierz opcję Reklamy
- Naciśnij „Usuń identyfikator reklamowy”
- Potwierdź, dotykając opcji „Wyczyść identyfikator reklamowy”

Identyfikator reklamowy jest teraz wyłączony; profilowanie nie jest już możliwe.

Więcej informacji na temat identyfikatora reklamowego można znaleźć na DB Planet tutaj:

> [#Mobile Workplace](#)

7 Najważniejsze aplikacje na początek

Najważniejsze aplikacje DB i aplikacje związane z pracą są już zainstalowane na Twoim urządzeniu.

7.1 Pobierz nowe aplikacje DB

Jeśli chcesz zainstalować więcej **aplikacji DB**, pobierz je ze **sklepu DB Google Play**. Aplikacje przeznaczone specjalnie dla DB, takie jak Meine DB, DB Planet i wiele innych, są dostępne do pobrania wyłącznie w tym sklepie.

Private Apps



u.a. Play Store, Galerie

Dienstliche Apps



Możesz pobrać **osobiste aplikacje** na swój **telefon Samsung/HMD** za pośrednictwem **sklepu Google Play** w sekcji prywatnej.

7.2 Aplikacja DB MOBIL Info

Zapomniałeś hasła blokady ekranu lub nie pamiętasz hasła użytkownika DB? Czy program Outlook ciągle się zawiesza? Czy pojawiają się komunikaty o błędach, których nie rozumiesz? Nie martw się, tutaj znajdziesz pomoc.



Aplikacja DB MOBIL to pierwsze miejsce, do którego należy się zwrócić w przypadku pytań dotyczących smartfona lub tabletu.

Funkcje na ekranie głównym:

- Zrób zrzut ekranu i zapisz go automatycznie w galerii służbowej lub aplikacji do zdjęć
- Odczytaj tagi NFC i wykorzystaj je w obszarze roboczym
- Używaj skanera kodów QR, aby uzyskać informacje związane z pracą
- Naciśnij lupę, aby przejść bezpośrednio do wyszukiwarki DB, gdzie możesz zadawać pytania dotyczące tematów związanych z DB

W zakładce „Instrukcje” znajdziesz najważniejsze przewodniki. W zakładce „Serwis” znajdziesz ważne linki związane z pracą oraz wszystkie linki osobiste potrzebne do pracy w DB, a także numer telefonu IT ServiceDesk.

Jeśli Twoje urządzenie obecnie nie działa, skorzystaj z urządzenia kolegi.

> Alternatywnie wszystkie ważne przewodniki można również znaleźć pod adresem: db.de/ae

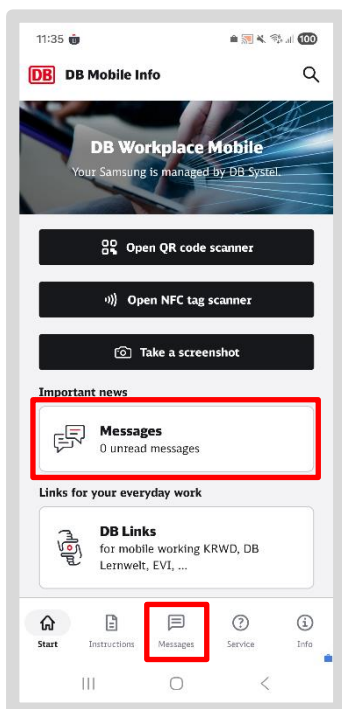


7.2.1 Powiadomienia push

Poprzez aplikację DB MOBIL będziesz otrzymywać **powiadomienia push** o nowych aktualizacjach oprogramowania lub innych sprawach związanych z Twoim urządzeniem. Na przykład poinformujemy Cię o dystrybucji i automatycznej instalacji oprogramowania na Twoim smartfonie lub tablecie.

Wszystkie informacje na temat Mobile Workplace i aplikacji DB MOBIL można znaleźć tutaj:

> [#Mobile Workplace](#)



Tutaj znajdziesz swoje wiadomości:

- Otwórz aplikację DB MOBIL. Na ekranie głównym zobaczysz obszar powiadomień
- Jeśli masz nową wiadomość, obok pozycji „Nieprzeczytane wiadomości” pojawi się mała czerwona cyfra
- Aby przeczytać wiadomości, dotknij sekcji „Wiadomości” u góry pośrodku lub zakładki „Wiadomości” na dole:

Więcej informacji znajdziesz tutaj:

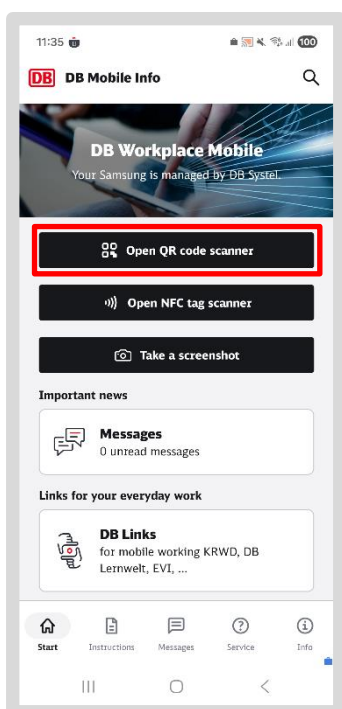
> [Aplikacja DB MOBIL: Odbieranie wiadomości](#)

7.2.2 Skanowanie kodów QR

Kody QR to czarno-białe kwadraty. Są to kody odczytywane elektronicznie. Specjalny czytnik dekoduje ten kod i przekierowuje Cię bezpośrednio do aplikacji lub dalszych informacji.

Oficjalne kody QR można skanować za pomocą aplikacji DB MOBIL na smartfonie lub tablecie:

- Otwórz aplikację DB MOBIL Info
- Naciśnij „Otwórz skaner kodów QR” i zezwól aplikacji na robienie zdjęć i nagrywanie filmów
- Otworzy się małe okienko, w którym można zeskanować kod QR. W tym celu należy umieścić kod QR w prostokącie
- Po zeskanowaniu kodu nastąpi przekierowanie na stronę internetową



7.3 Outlook

Dzięki programowi Outlook możesz odbierać i wysyłać służbowe wiadomości e-mail. Zanim zaczniesz, musisz skonfigurować kilka ustawień.

- Masz pytania dotyczące pisania i wysyłania wiadomości e-mail? Na [stronie IT fit](#) znajdziesz przydatne wskazówki i poradniki dotyczące korzystania z programu Outlook.

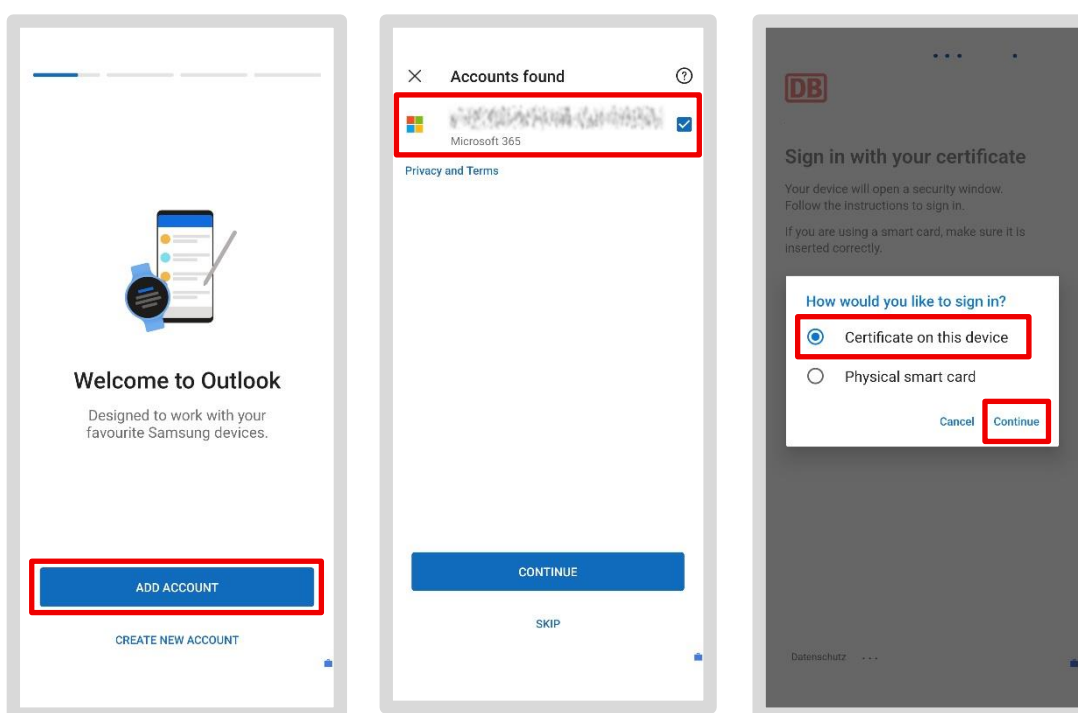
7.3.1 Konfiguracja programu Outlook / Utworzenie konta e-mail / Konfiguracja szyfrowania wiadomości e-mail

> **Uwaga:** Film instruktażowy znajdziesz na stronie db.de/mobile-videoanleitung

- Przejdź do obszaru „Praca” i dotknij aplikacji „Outlook”
- Twoje konto e-mail powinno być już skonfigurowane automatycznie – dotknij „Dodaj konto”
- W następnym kroku wybierz swój adres e-mail i kliknij „Dalej”

Po wyświetleniu monitu o zalogowanie się może pojawić się prośba o podanie tymczasowej legitymacji pracownika DB (TAP):

- Jeśli tymczasowa legitymacja pracownika DB jest nadal ważna, wprowadź ją tutaj lub utwórz nową zgodnie z opisem w [rozdziale 4.6 Aktywacja urządzenia – Utwórz tymczasową legitymację pracownika DB \(TAP\)](#)
- Alternatywnie: w sekcji „Wybierz inną opcję logowania” wybierz opcję „Certyfikat na tym urządzeniu”
- Naciśnij „Wybierz”, gdy pojawi się prośba o certyfikat



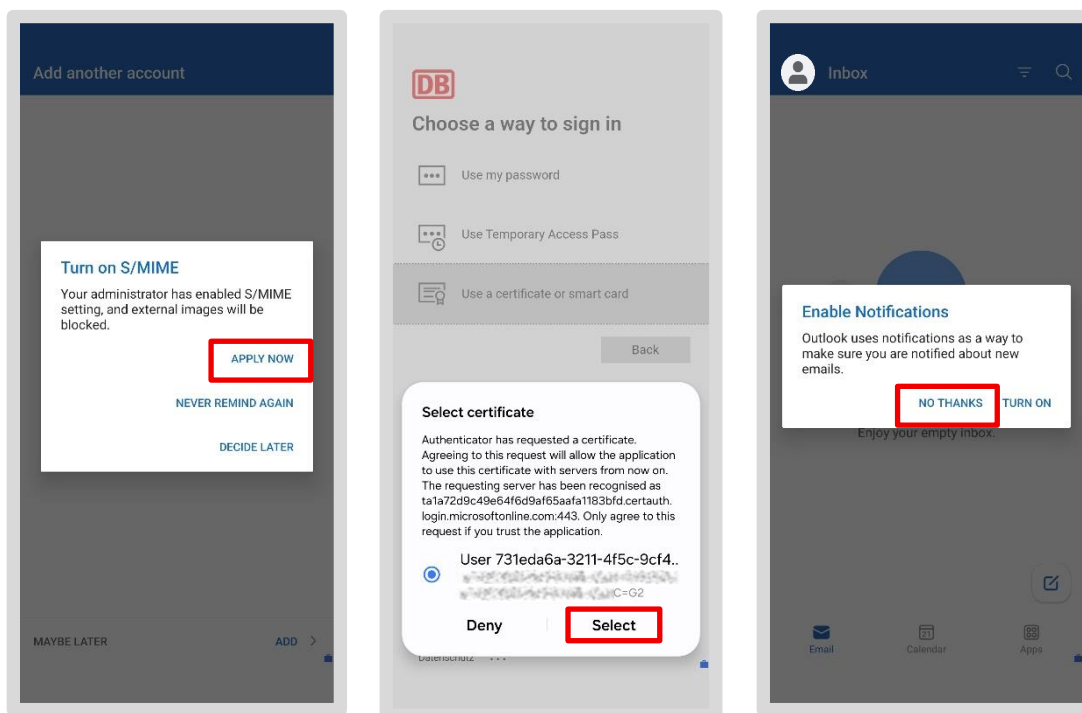
- Jeśli chcesz wysłać pocztą elektroniczną dane wymagające specjalnej ochrony (np. dane osobowe), musisz również zastosować szyfrowanie treści wiadomości
- DB zapewnia w tym celu szyfrowanie S/MIME
- Naciśnij „Zastosuj teraz”, gdy pojawi się pytanie, czy chcesz aktywować S/MIME

Następnie pojawi się monit o certyfikat. Certyfikat, który jest dla Ciebie ważny, możesz zidentyfikować w następujący sposób:

- Pierwsza linia: „**User** ds2232... (po czym następują cyfry i litery)
- Drugi wiersz: „CN- Nazwa **użytkownika bazy** danych”, np. LisaMustermann89sd7es0ßwd (po której następują cyfry i litery)
- Zaznacz fragment tekstu i naciśnij „Wybierz”

Twoje konto e-mail jest teraz konfigurowane:

- Naciśnij „Może później”, gdy pojawi się pytanie, czy chcesz dodać kolejne konto
- Następnie naciśnij „Nie, dziękuję”, aby wyłączyć powiadomienia



- Twoje wiadomości e-mail są teraz ładowane (proces ten może potrwać kilka minut)
- Możesz teraz ponownie czytać i tworzyć wiadomości e-mail

Android 16: Na urządzeniach z systemem Android 16 można pominąć krok aktywacji S/MIME. W takim przypadku musisz zakończyć konfigurację Outlooka i ponownie uruchomić aplikację! Pojawi się wtedy monit o aktywację.

7.3.2 Konfiguracja podpisu e-mailowego

Podpisy e-mailowe są obowiązkowym elementem komunikacji biznesowej. Pojawiają się one na końcu wiadomości e-mail i zgodnie z prawem muszą zawierać określone informacje, takie jak nazwa firmy oraz oficjalna siedziba firmy zarejestrowanej w DB. Tekst podpisu e-mailowego można znaleźć w centralnym katalogu DB, znanym jako „EVI”.

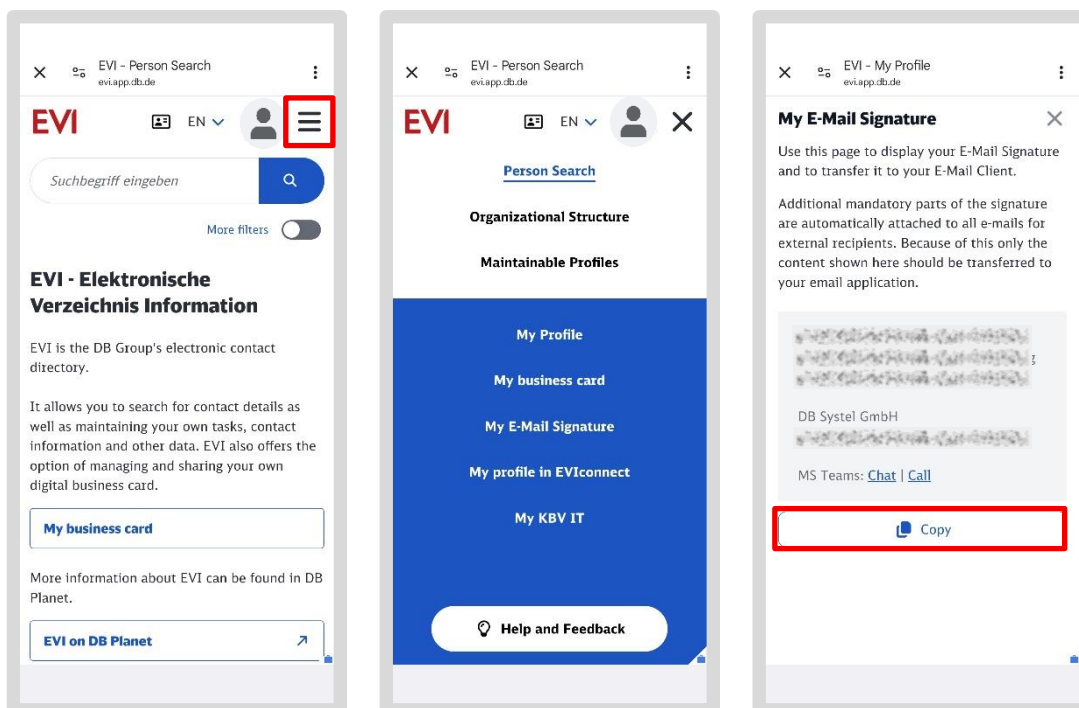
Oto jak pobrać podpis e-mailowy z EVI:




- Otwórz aplikację EVI w sekcji „Praca/Biznes”
- Zobaczysz teraz widok mobilnej aplikacji EVI
- Naciśnij menu w lewym górnym rogu, a następnie wybierz „Nowe EVI”

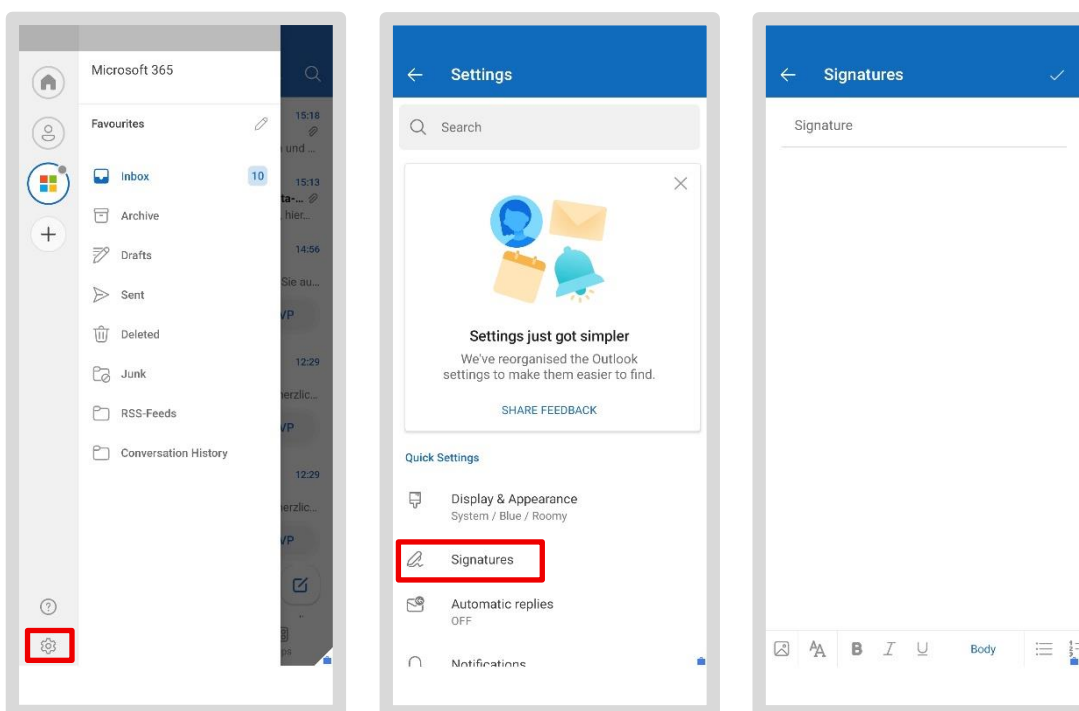
Otworzy się widok nowego EVI:

- Naciśnij trzy linie obok swojego zdjęcia profilowego w prawym górnym rogu
- Następnie dotknij „Mój podpis e-mailowy”
- Otworzy się strona „Mój podpis e-mailowy”
- Twój osobisty podpis jest wyświetlony w szarym polu. Skopiuj go, dotykając przycisku „Kopiuj” na dole
- Następnie zamknij EVI



Wklej podpis do Outlooka:

- Otwórz aplikację Outlook w sekcji „Praca/Biznes”
- Naciśnij swoje zdjęcie profilowe w lewym górnym rogu
- Po lewej stronie otworzy się przegląd folderów poczty
- Naciśnij ikonę koła zębatego w lewym dolnym rogu 
- Teraz dotknij „Podpisy”
- Otworzy się pole na podpis. Jeśli jest tam już wpis, usuń go, dotykając opcji „✕”



- Teraz naciśnij i przytrzymaj puste pole, aż pojawi się opcja „Wklej”, a następnie ją wybierz
- Twoja skopiowana sygnatura z EVI zostanie wstawiona
- Zamknij okno – Twój podpis będzie teraz automatycznie wstawiany do wszystkich pisanych przez Ciebie wiadomości e-mail

Uwaga: Jeśli skonfigurowałeś wiele kont e-mail, możesz użyć suwaka „Podpis dla każdego konta”, aby ustawić oddzielny podpis dla każdego konta. W przeciwnym razie zapisany podpis będzie używany dla wszystkich Twoich kont e-mail.

7.3.3 Synchronizacja wiadomości e-mail – wszystkie wiadomości zawsze aktualne

Wszystkie Twoje wiadomości e-mail są automatycznie archiwizowane w aplikacji Outlook i synchronizowane z połączonym kontem Office. Oznacza to, że bez względu na to, z jakiego urządzenia się logujesz – czy to ze smartfona, tabletu, czy komputera BKU/Basic Workplace – zawsze masz aktualne dane.

Jeśli posiadasz stary smartfon lub tablet i chcesz zaimportować kontakty, przejdź do [sekcji 8.5: Tworzenie kopii zapasowej kontaktów w usłudze OneDrive](#).

7.3.4 Tworzenie nowych kontaktów w programie Outlook

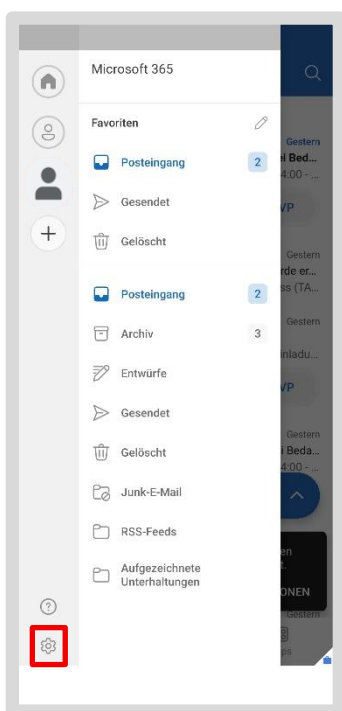


- Przejdź do sekcji „Praca” i otwórz aplikację Kontakty
- Naciśnij „+”, aby utworzyć nowy kontakt
- Wybierz „Outlook” w lewym górnym rogu nad strzałką
- Nowy kontakt zostanie zapisany w programie Outlook

7.3.5 Synchronizacja kontaktów w programie Outlook

Jeśli utworzysz nowy kontakt w obszarze „Praca/Biznes” na smartfonie lub tablecie za pomocą aplikacji Kontakty, zaleca się udostępnienie go w celu synchronizacji z Outlookiem. Oto jak to zrobić:

- Otwórz *aplikację Outlook* w sekcji „Praca/Biznes”
- W lewym górnym rogu aplikacji znajduje się okrąg z ikoną. Naciśnij go
- Po lewej stronie otworzy się przegląd folderów poczty e-mail



- Wybierz ikonę koła zębatego w lewym dolnym rogu

- Otworzą się ustawienia
- W sekcji „Konta e-mail” wybierz swoje konto Outlook. Następnie dotknij małego suwaka obok opcji „Synchronizuj kontakty”
- Następnie potwierdź żądanie dostępu, dotykając „Zezwól”
- Po włączeniu synchronizacji zamknij aplikację Outlook

7.4 Aplikacja MS Defender – musi być otwarta

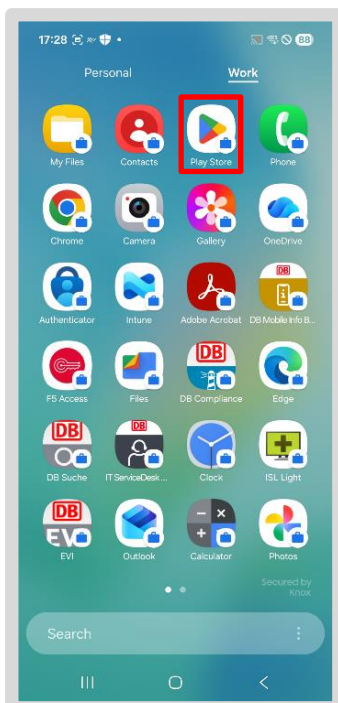
Po włączeniu aplikacji Outlook i Teams włącz aplikację „Microsoft Defender for Endpoint Mobile” (w skrócie aplikacja MS Defender) na swoim smartfonie/tablecie. Aplikacja chroni przed cyberatakami i skanuje istniejące aplikacje w poszukiwaniu złośliwego oprogramowania. Aby aktywować ochronę, otwórz aplikację raz.

Ze względu na dużą różnorodność smartfonów/tabletów mogą występować niewielkie różnice w opisie poszczególnych kroków.

7.4.1 Konfiguracja aplikacji MS Defender

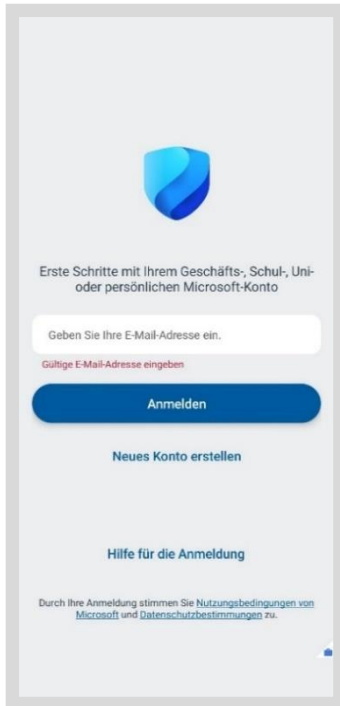
Aby skonfigurować aplikację MS Defender na smartfonie/tablecie, należy wykonać następujące czynności:

- Przejdź do sekcji Praca/Biznes i otwórz „DB Google Play Store”

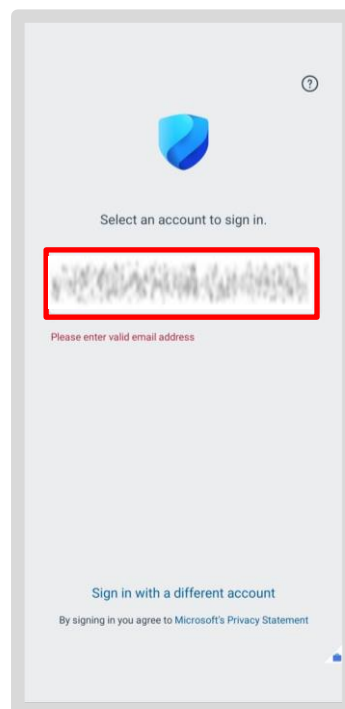
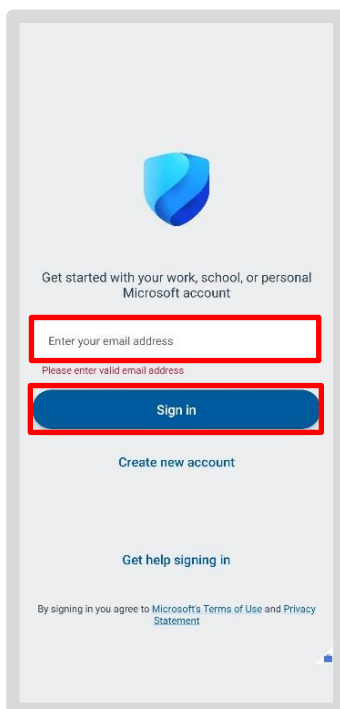


- Wyszukaj aplikację „Microsoft Defender: Antivirus” i naciśnij „Zainstaluj”

- Naciśnij ikonę aplikacji „MS Defender”, aby ją otworzyć



- Zostaniesz poproszony o podanie służbowego adresu e-mail
- Naciśnij przycisk „Zaloguj się”, w przeciwnym razie aplikacja automatycznie przeniesie Cię do następnego ekranu, na którym wyświetli się Twój adres e-mail
- Wybierz swój służbowy adres e-mail

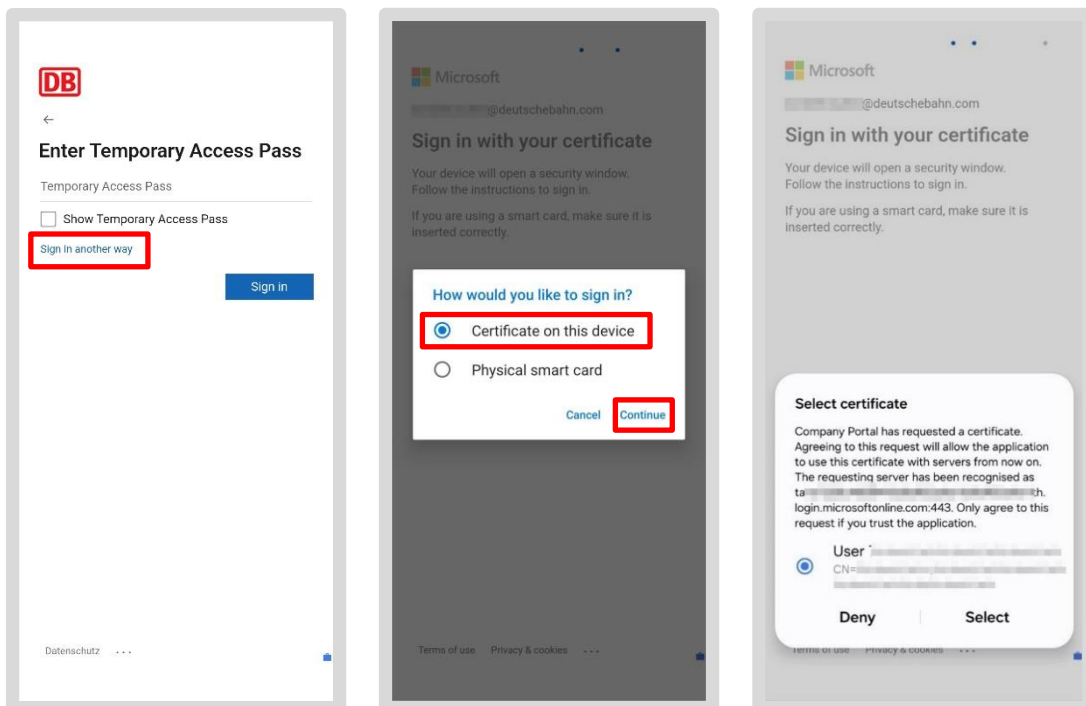


Jeśli w ciągu ostatniej godziny aktywowałeś smartfon/tablet za pomocą aplikacji Intune, możesz zostać poproszony o ponowne wprowadzenie tymczasowej legitymacji pracownika DB.

- Naciśnij „Zaloguj się w inny sposób”

Następnie kontynuuj:

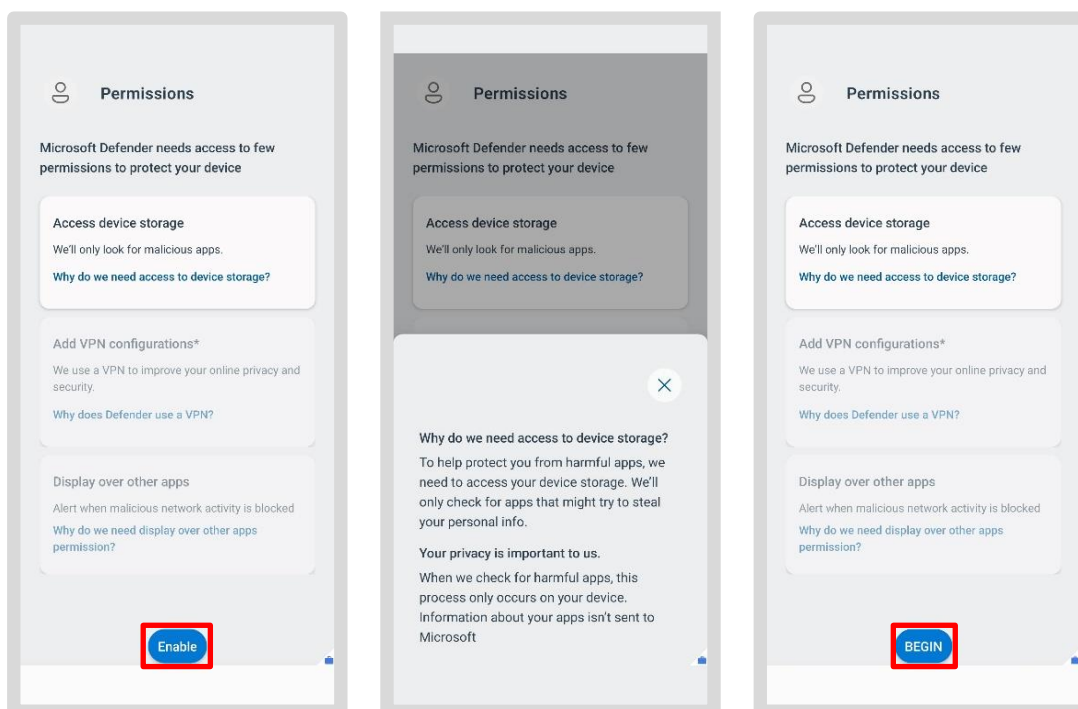
- Gdy pojawi się monit, wybierz opcję „Certyfikat na tym urządzeniu”, a następnie „Dalej”
- Wybierz certyfikat



7.4.2 Przyznaj uprawnienia

Aplikacja poprosi Cię teraz o niezbędne uprawnienia. W tym momencie kolejność ekranów może różnić się od tej przedstawionej w instrukcji. Jeśli pierwszy ekran wygląda tak jak na ilustracji:

- Naciśnij „Aktywuj”
- Następnie dotknij „Start”
- Otworzy się aplikacja „Ustawienia” na smartfonie/tablecie

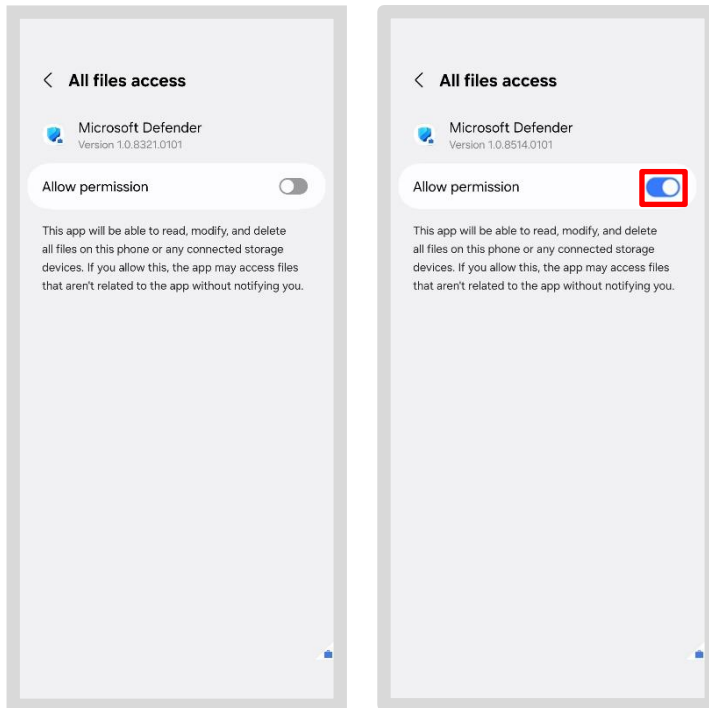


Informacje ogólne dotyczące uprawnień:

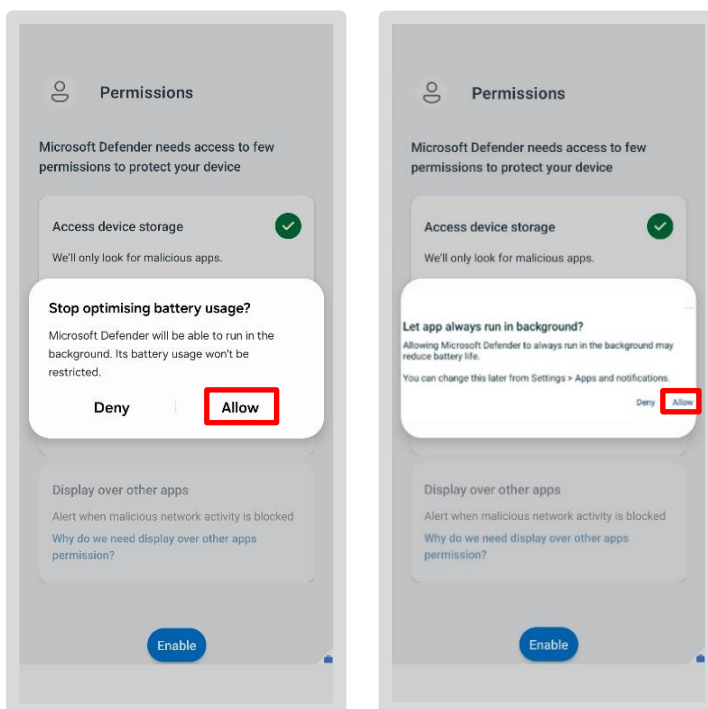
Uprawnienia te są wymagane, aby zapewnić prawidłowe działanie aplikacji i zagwarantować bezpieczeństwo urządzenia.

Możesz wyświetlić okno informacyjne dla każdego uprawnienia (np. dotycząc „Dlaczego potrzebujemy dostępu do pamięci urządzenia?”). Niektóre pozycje nie mogą jednak zostać wybrane (są wyszarzone, np. „Dodaj konfigurację VPN”) lub są już włączone (zielony haczyk, np. „Uruchom w tle”), ponieważ są one zdefiniowane przez system.

- Teraz przesunij suwak w prawo, aby przyznać uprawnienie
- W kolejnym oknie dialogowym dotknij „Zezwól”



- W kolejnych okienkach kliknij „Zezwól”

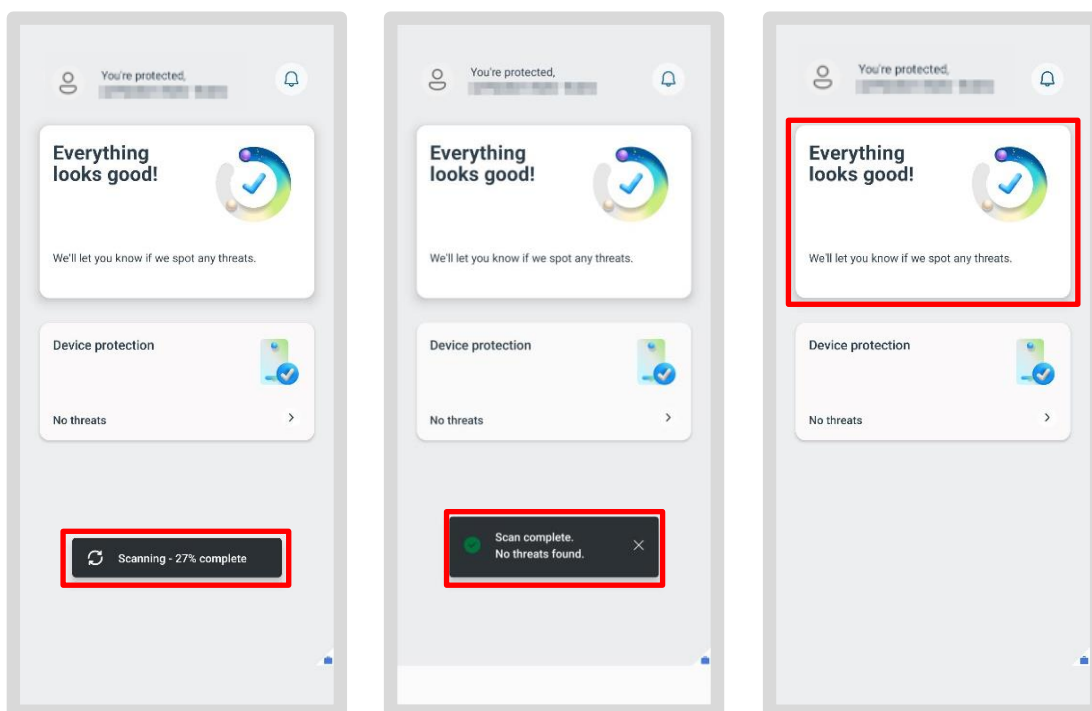


Uwaga: W zależności od typu urządzenia mogą zostać wyświetlone inne prośby o uprawnienia! W rezultacie może zostać wyświetlony tylko jeden z pokazanych ekranów.

Następnie zostaniesz przeniesiony do ekranu głównej aplikacji MS Defender. Skanowanie w poszukiwaniu złośliwego oprogramowania na smartfonie/tablecie zostanie

przeprowadzone automatycznie od razu. Podczas skanowania będą wyświetlane aktualizacje postępu.

Wynik zostanie wyświetlony na ekranie głównym. Jeśli widoczny jest zielony haczyk, oznacza to, że nie wykryto złośliwego oprogramowania.



Gratulacje!

Pomyślnie zakończyłeś konfigurację początkową! Urządzenie jest teraz chronione przed złośliwym oprogramowaniem.

7.5 DB M 365

Możesz również otwierać i przeglądać pliki Word, Excel, PowerPoint lub PDF na swoim smartfonie lub tablecie. W tym celu wystarczy jednorazowo pobrać odpowiednie aplikacje:

- Otwarcie sklepu DB Google Play
- Wyszukaj odpowiednią aplikację za pomocą paska wyszukiwania, na przykład Word, Excel, PowerPoint lub PDF Reader



- Następnie naciśnij „Zainstaluj”. Aplikacja zostanie pobrana i pojawi się w sekcji „Praca/Biznes”
- Po otwarciu pliku aplikacja uruchomi się automatycznie

Uwaga: Można otworzyć tylko jeden plik na raz. Nie jest możliwe, na przykład, otwarcie kilku plików Word jednocześnie.

7.6 Aplikacja Microsoft Authenticator

Aplikacja Microsoft Authenticator umożliwia **uwierzytelnianie wieloskładnikowe (MFA)**.

Aplikacja Microsoft Authenticator będzie potrzebna na przykład do:

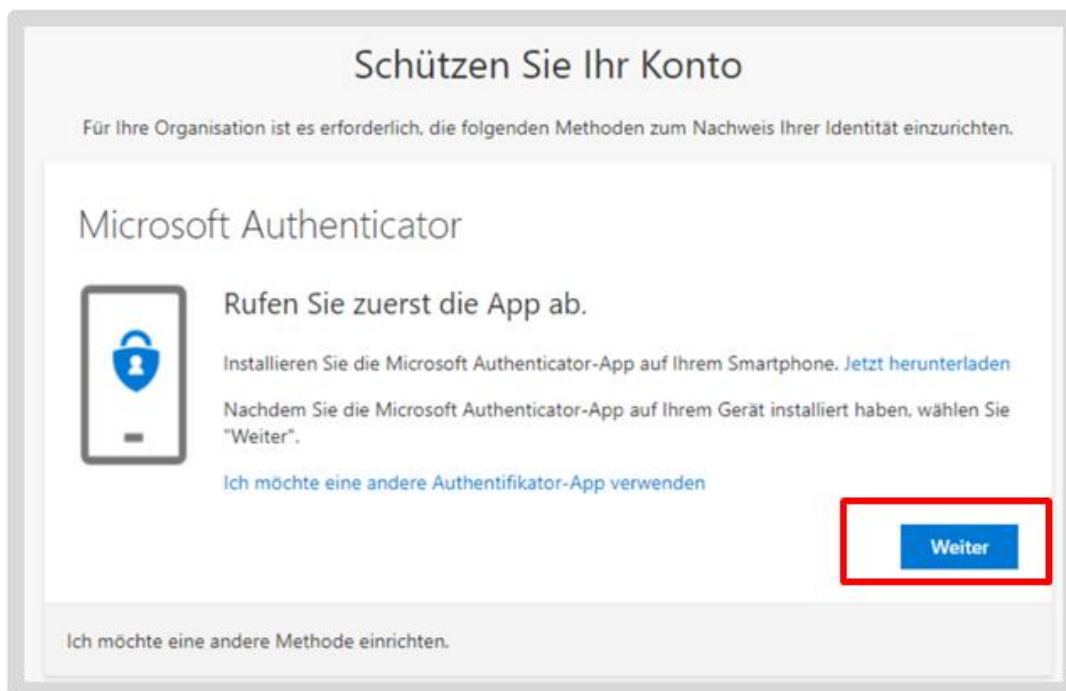
- Połączenie VPN z Basic Workplace MAC
- Korzystanie z konta administratora bazy danych
- uzyskania dostępu do określonych aplikacji, np. SAP



Rozróżnia się, czy korzystałeś już z aplikacji Microsoft Authenticator na smartfonie lub tablecie z systemem DB, czy też używasz tej aplikacji na swoim smartfonie lub tablecie po raz pierwszy.

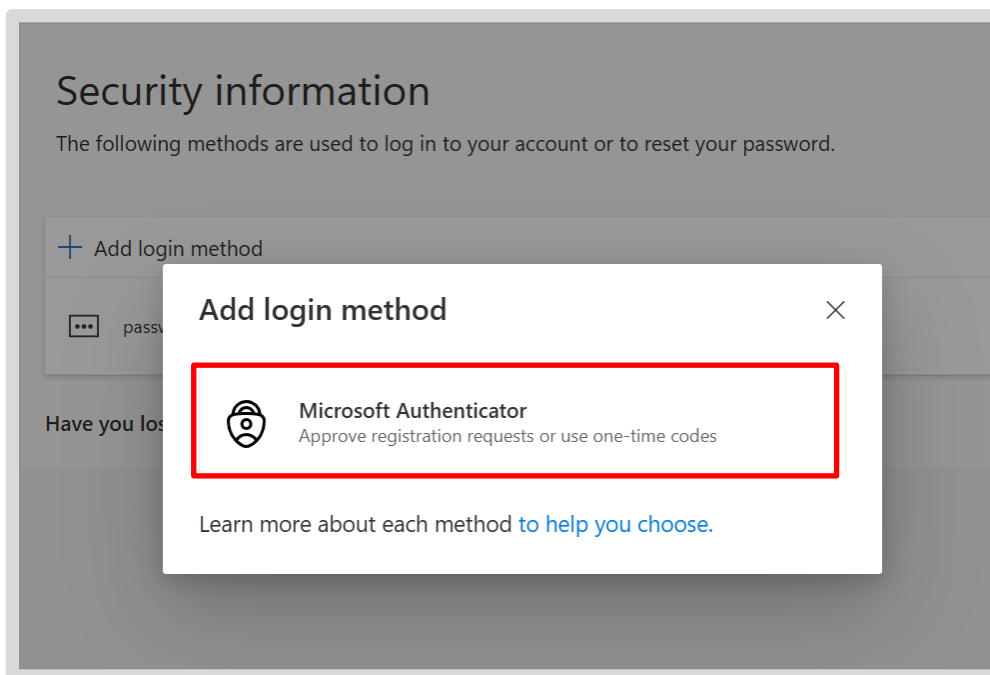
Pierwsze użycie aplikacji do uwierzytelniania Microsoft Authenticator

Po dotknięciu aplikacji wymagającej aplikacji Microsoft Authenticator otworzy się to okno dialogowe. Dotknij „Kontynuuj” i postępuj zgodnie z instrukcjami krok po kroku; w tym celu dotknij przycisku „Przewodnik uwierzytelniania MFA”



Możesz też samodzielnie uruchomić aplikację do uwierzytelniania Microsoft Authenticator:

- Naciśnij „db.de/authenticator” na komputerze BKU lub Basic Workplace
- Naciśnij „ikonę plusa” i przycisk „Dodaj metodę logowania”
- Otworzy się okno dialogowe; wybierz „Microsoft Authenticator”



- Przejdź na smartfon/tablet i otwórz aplikację Microsoft Authenticator do uwierzytelniania
- Otwórz tę stronę, aby uzyskać instrukcje krok po kroku, dotknij przycisku „Przewodnik konfiguracji MFA” i postępuj zgodnie z podanymi instrukcjami
- Następnie możesz używać aplikacji Microsoft Authenticator do uwierzytelniania na swoim smartfonie/tablecie

Przechodzenie ze starego na nowy smartfon/tablet z systemem DB

Jeśli korzystałeś już z aplikacji Microsoft Authenticator do uwierzytelniania, pamiętaj o następujących kwestiach:

- Jeśli musisz użyć aplikacji Authenticator podczas konfiguracji nowego smartfona/tabletu, użyj starego smartfona/tabletu, aby połączyć go z aplikacją Authenticator
- Otwórz tę instrukcję krok po kroku, naciśnij przycisk „Przewodnik po konfiguracji uwierzytelniania wieloskładnikowego” i postępuj zgodnie z podanymi instrukcjami
- Następnie możesz używać aplikacji Microsoft Authenticator na nowym smartfonie/tablecie i zresetować stary smartfon/tablet. Jeśli korzystałeś z aplikacji Authenticator w witrynach internetowych lub narzędziach, ponownie aktywuj aplikację w

- **Wskazówka:** Jeśli masz trudności z ponowną aktywacją połączeń w aplikacji Authenticator po przywróceniu, skorzystaj z portalu samoobsługowego pod adresem semdb.de/resetmfa i postępuj zgodnie z instrukcjami od początku do końca

7.7 Podsumowanie: aplikacje DB

Gdzie mogę znaleźć aplikacje DB?

Najważniejsze aplikacje są już zainstalowane na Twoim służbowym smartfonie/tablecie. Jeśli chcesz pobrać kolejne aplikacje służbowe, zrób to za pośrednictwem **sklepu DB Google Play**.

Znajdziesz tam na przykład Outlook, Word i OneDrive, a także aplikacje specyficzne dla DB, takie jak Meine DB lub DB Planet.

Aplikacje osobiste można pobrać za pośrednictwem sklepu Google Play.

Gdzie mogę znaleźć informacje o moim smartfonie/tablecie?

W przypadku jakichkolwiek pytań dotyczących smartfona/tabletu skorzystaj z aplikacji DB MOBIL. W zakładce „Instrukcje” znajdziesz przewodniki, a w zakładce „Serwis” przydatne informacje o swoim urządzeniu.

Aplikacja jest domyślnie zainstalowana na smartfonie/tablecie.

8 Tworzenie kopii zapasowej d

8.1 Tworzenie kopii zapasowej danych służbowych w OneDrive

Posiadasz smartfon/tablet z wersją Enterprise. Oznacza to, że dokumenty służbowe i osobiste są ściśle oddzielone, jeśli chodzi o tworzenie kopii zapasowych.

Sposób tworzenia kopii zapasowych dokumentów prywatnych lub zdjęć/filmów opisano tutaj:

- > [mobileworkplace.deutschebahn.com/mobile-zabezpieczanie danych](https://mobileworkplace.deutschebahn.com/mobile-zabezpieczanie-danych)
- > **Uwaga:** Film instruktażowy znajdziesz na stronie db.de/mobile-videoanleitung

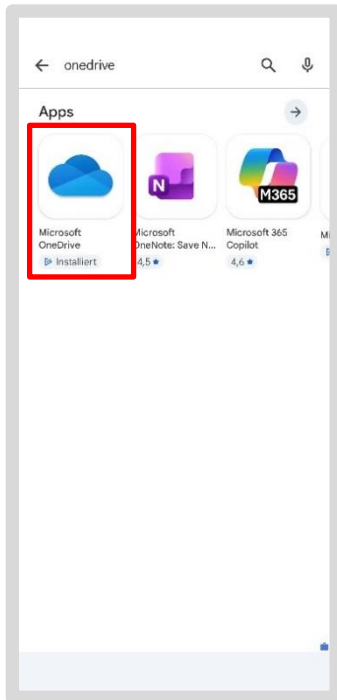
Aby zapisywać zdjęcia i inne dokumenty, takie jak pliki PDF lub Word, potrzebna jest aplikacja Microsoft „OneDrive”. Dzięki tej aplikacji możesz przechowywać wszystkie dane związane z pracą w chmurze, a następnie uzyskać do nich dostęp w dowolnym momencie ze wszystkich urzędzeń służbowych. Oznacza to, że możesz na przykład uzyskać dostęp do swoich danych z firmowego komputera.



8.2 Konfiguracja OneDrive

Wymagania wstępne: Aby skonfigurować OneDrive, najpierw zainstaluj aplikację Outlook na swoim smartfonie/tablecie i skonfiguruj swoje służbowe konto e-mail. Więcej informacji na temat konfiguracji znajdziesz w [rozdziale 7.3 Outlook](#).

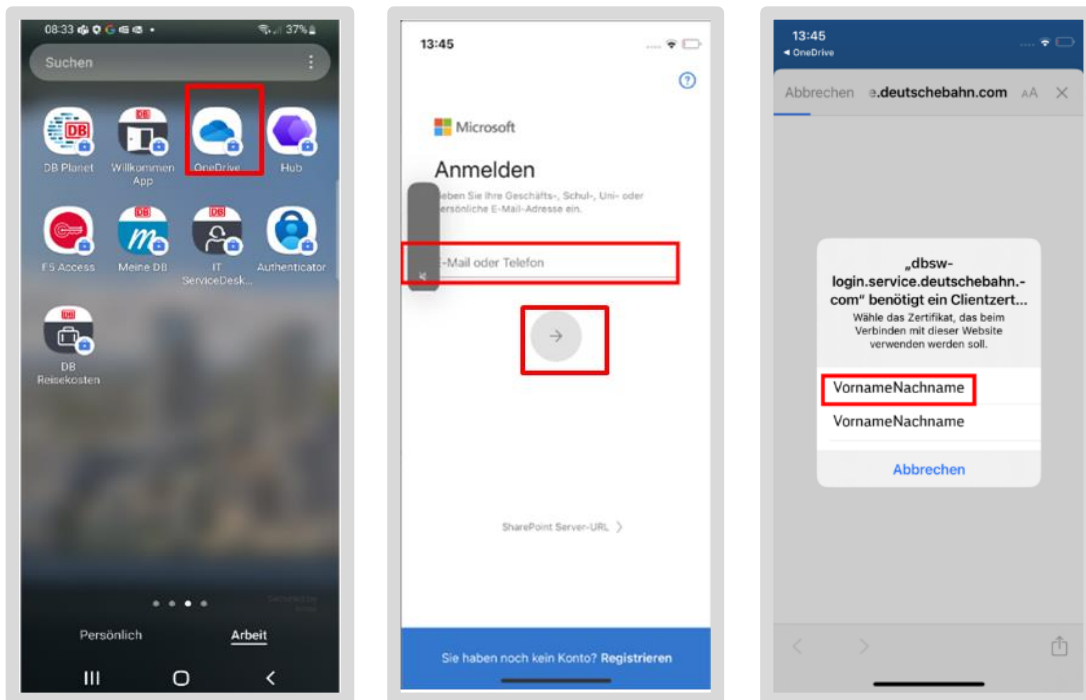
- Trzymaj tablet w orientacji pionowej, aby ekrany odpowiadały układowi przedstawionemu w instrukcji
- Pobierz aplikację „OneDrive”. W tym celu otwórz sklep Google Play
- Wyszukaj aplikację „Microsoft OneDrive”



8.2.1 Android 15

Po zainstalowaniu aplikacja pojawi się jako ikona (wskazówka: chmura) o nazwie OneDrive w sekcji „Praca/Biznes” na ekranie głównym smartfona/tabletu.

- Otwórz *aplikację OneDrive*, dotykając ikony
- Potwierdź, że aplikacja ma pozwolenie na wysyłanie powiadomień
- Wybierz „**Zaloguj się**”
- Wprowadź swój adres e-mail DB – zostaniesz zalogowany automatycznie
- Wybierz swój certyfikat użytkownika DB
- Teraz zobaczysz wszystkie swoje pliki w OneDrive
- Wprowadź swój adres e-mail DB – zostaniesz zalogowany automatycznie
- Wybierz swój certyfikat użytkownika DB



Uwaga: Jeśli konfigurujesz OneDrive po raz pierwszy, synchronizacja wszystkich danych może potrwać kilka minut.

Tworzenie kopii zapasowej wszystkich ustawień systemowych

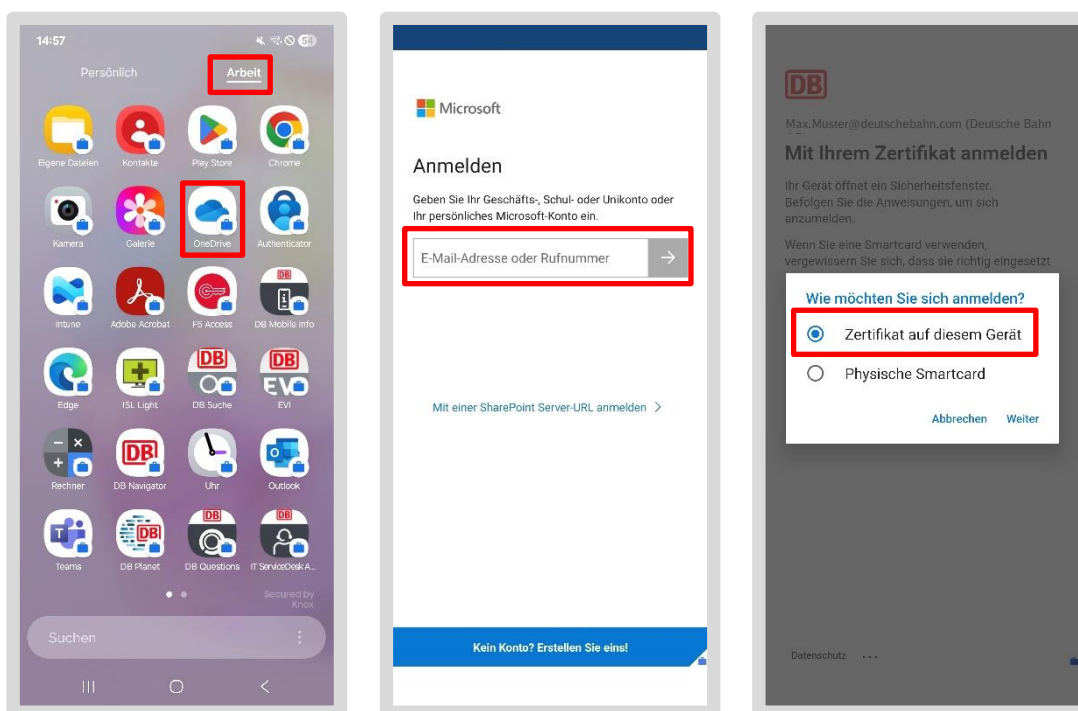
Jeśli kiedykolwiek zajdzie potrzeba przywrócenia ustawień fabrycznych smartfona/tabletu, pamiętaj o utworzeniu kopii zapasowej ustawień systemowych.

Zrób zrzuty ekranu lub zanotuj swoje indywidualne ustawienia oraz konkretne aplikacje DB związane z pracą. Zapisz je również w OneDrive, abyś mógł odwołać się do nich jako notatek podczas procesu renowacji.

8.2.2 Android 16

Po instalacji aplikacja pojawi się jako ikona (wskazówka: chmura) o nazwie OneDrive w obszarze „Praca/Biznes” na ekranie głównym smartfona/tabletu.

- Otwórz aplikację *OneDrive*, dotykając ikony
- Potwierdź, że aplikacja ma uprawnienia do wysyłania powiadomień
- Wybierz „Zaloguj się”
- Wprowadź swój adres e-mail DB i potwierdź, dotykając niebieskiej strzałki
- Następnie wybierz swój certyfikat użytkownika DB z opcji „*Certyfikat na tym urządzeniu*”
- Potwierdź, dotykając „Wybierz”



Teraz możesz zobaczyć wszystkie pliki, które zapisałeś w OneDrive.

Ważne: Jeśli po wybraniu certyfikatu ponownie pojawi się ekran logowania, wprowadź ponownie swój adres e-mail DB i spróbuj zalogować się jeszcze raz.

Uwaga: Jeśli konfigurujesz OneDrive po raz pierwszy, synchronizacja wszystkich danych może potrwać kilka minut.

Tworzenie kopii zapasowej wszystkich ustawień systemowych

Jeśli kiedykolwiek przywrócisz ustawienia fabryczne na swoim smartfonie/tablecie, pamiętaj, aby wykonać również kopię zapasową ustawień systemowych.

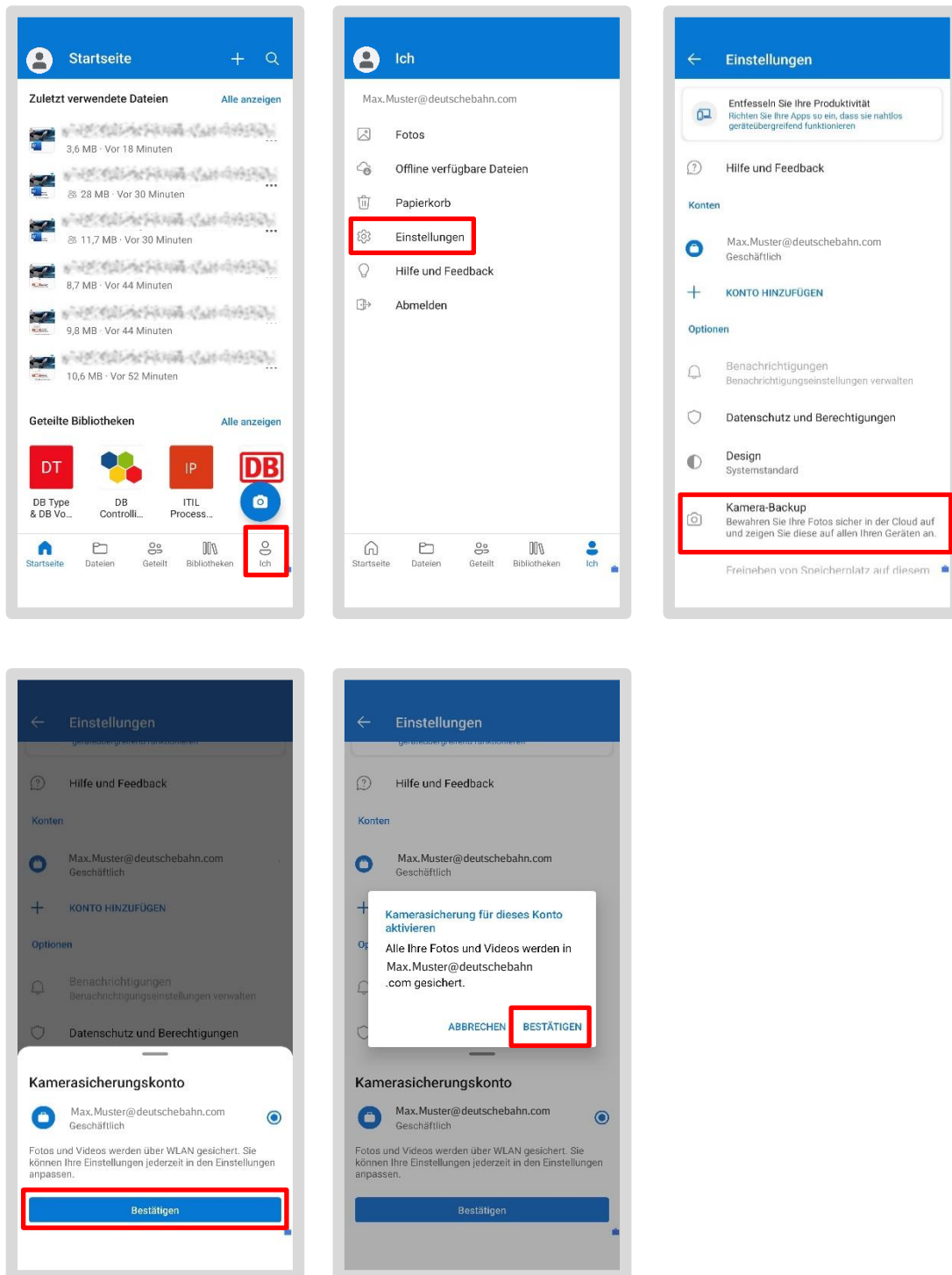
Wskazówka:

Zrób zrzuty ekranu lub sporządź notatki dotyczące indywidualnych ustawień oraz konkretnych aplikacji bazodanowych używanych w pracy. Zapisz je również w usłudze OneDrive, aby móc z nich korzystać jako notatek podczas procesu renowacji.

8.3 Tworzenie kopii zapasowej zdjęć

Jeśli chcesz automatycznie zapisywać zdjęcia w usłudze OneDrive, wykonaj następujące czynności:

- Otwórz aplikację *OneDrive*
- Naciśnij ikonę „Profil” w prawym dolnym rogu, a następnie wybierz „Ustawienia”
- Następnie wybierz „Kopia zapasowa z aparatu”
- Następnie dotknij dwukrotnie „Potwierdź”

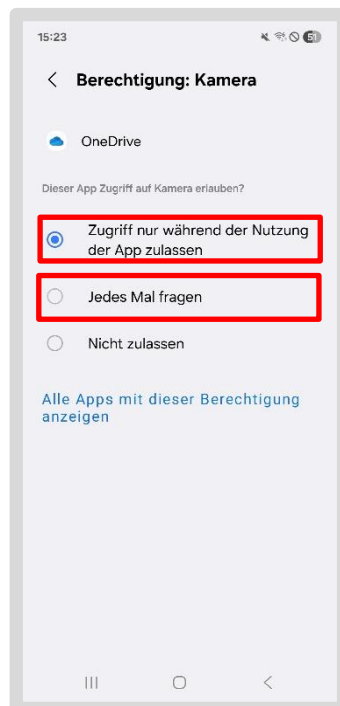
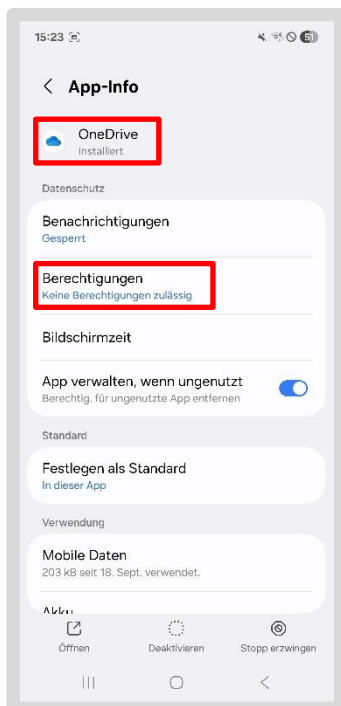


W następnym kroku musisz przyznać OneDrive uprawnienia dostępu do swoich zdjęć i aparatu. Aby to zrobić, wykonaj następujące czynności:

- Po dwukrotnym potwierdzeniu pojawi się komunikat o błędzie informujący, że OneDrive nie ma uprawnień
- Następnie naciśnij przycisk po prawej stronie oznaczony jako „Dostosuj ustawienia”.
- Zostaniesz przeniesiony do ustawień uprawnień aplikacji

Jeśli nie pojawi się komunikat o błędzie lub go zamknąłeś:

- Przejdź do sekcji „Aplikacje” w „Ustawieniach”
- Następnie wybierz aplikację OneDrive w sekcji „Praca”
- Naciśnij „Uprawnienia”
- Naciśnij raz „Aparat”, a następnie „Zdjęcia i filmy”, aby przyznać OneDrive uprawnienia
- Zdecyduj samodzielnie, czy chcesz, aby OneDrive pytał Cię za każdym razem, czy też chcesz przyznać stały dostęp podczas korzystania z aplikacji
- Po skonfigurowaniu synchronizacji każde zdjęcie zrobione aparatem zostanie zsynchronizowane z OneDrive



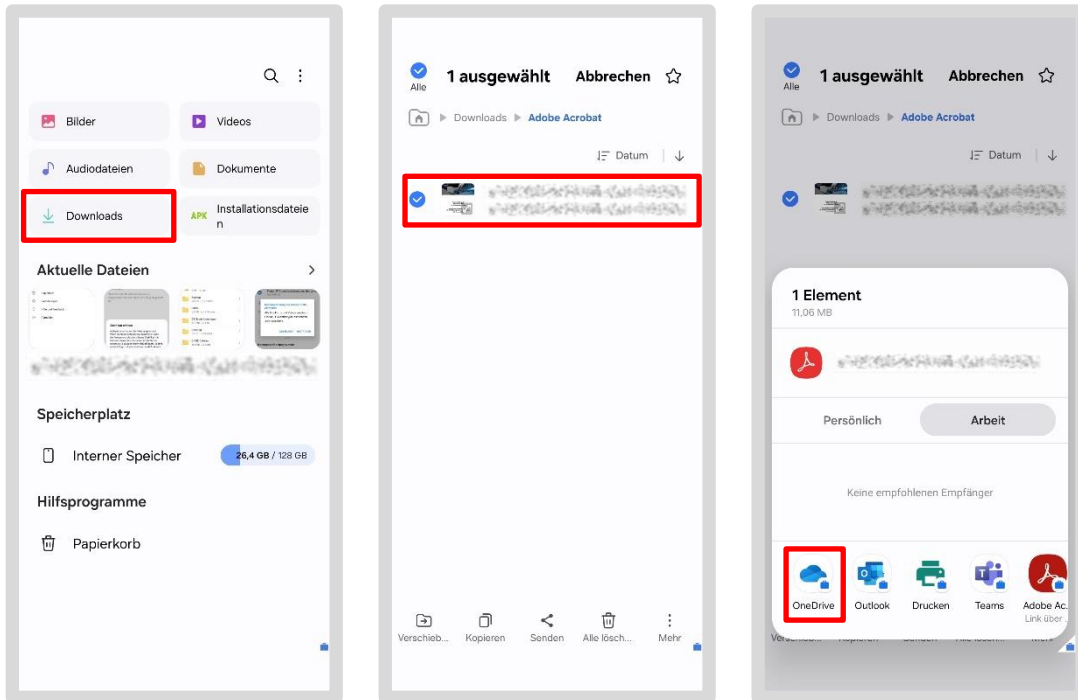
8.4 Tworzenie kopii zapasowych plików PDF

Pliki PDF są zazwyczaj zapisywane w folderze „Pobrane” w sekcji „Obszar roboczy”. Aby wykonać ich kopię zapasową w OneDrive, wykonaj następujące czynności:

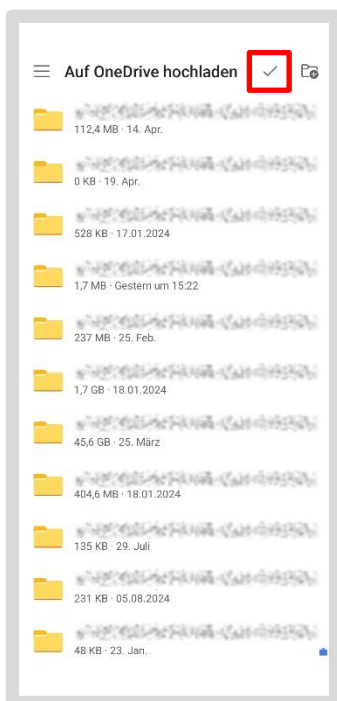
- Otwórz aplikację *Pliki*



- Naciśnij „Pobrane”
- Naciśnij i przytrzymaj plik PDF, aż obok nazwy pojawi się znacznik
- Naciśnij „Wyślij” na dole paska menu, a następnie wybierz „OneDrive”



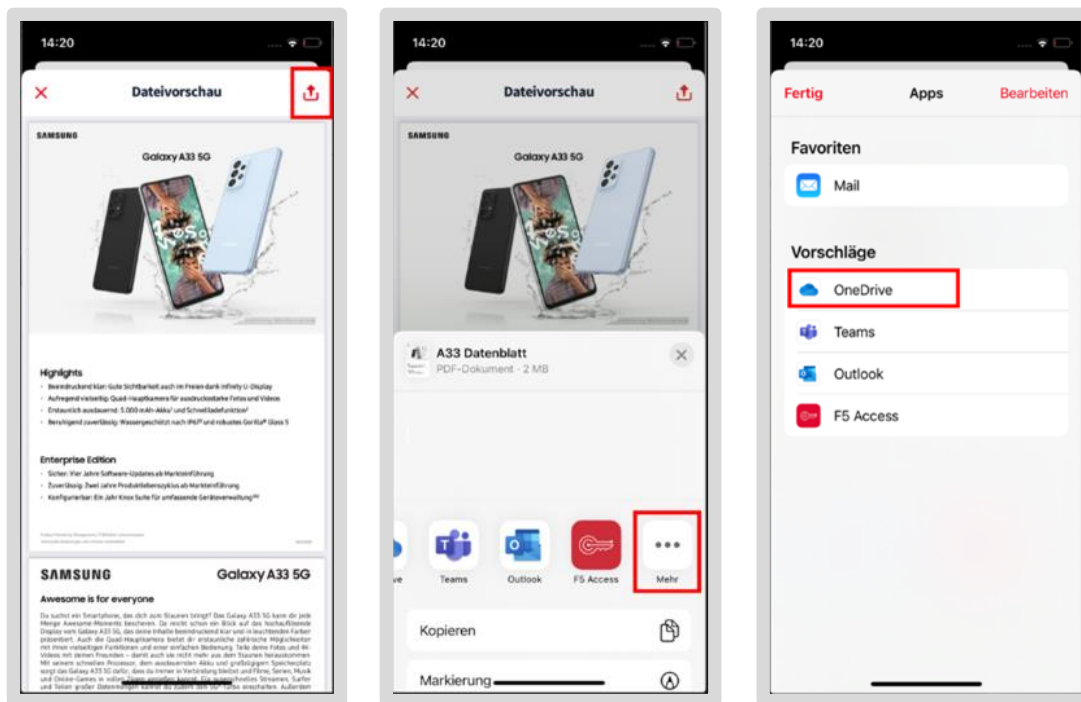
- Wyświetli się Twój osobisty folder w OneDrive
- Jeśli to nie jest właściwa lokalizacja: dotknij menu hamburgerowego (trzy poziome linie) w lewym górnym rogu
- Wybierz folder, w którym chcesz zapisać plik PDF, a następnie dotknij białego znacznika w prawym górnym rogu
- Plik zostanie teraz przesłany do OneDrive



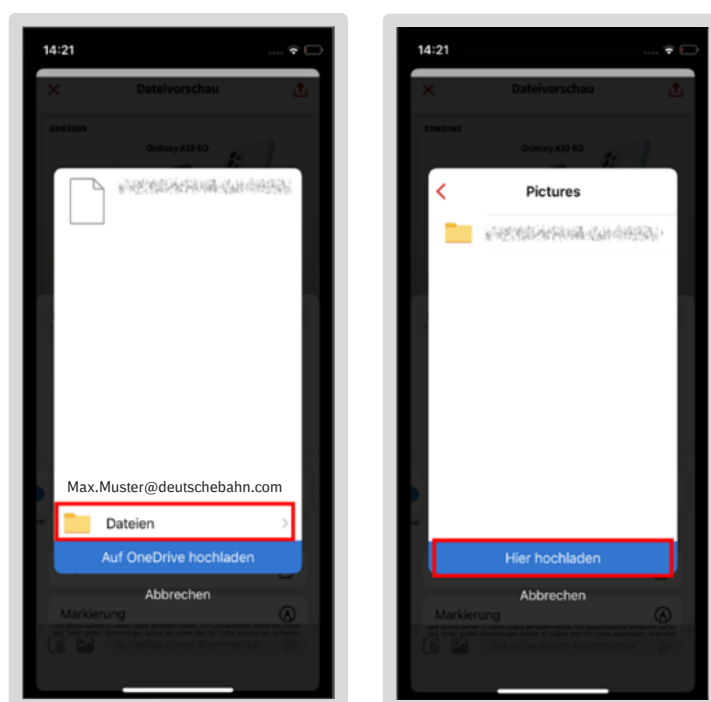
8.4.1 Zapisywanie plików PDF bezpośrednio w usłudze OneDrive

Pliki PDF można zapisywać bezpośrednio w OneDrive; wykonaj następujące czynności:

- Otwórz plik
- Naciśnij ikonę udostępniania w prawym górnym rogu
- Wybierz „OneDrive” z menu na dole (pod kropkami „...”)



- Wybierz folder, w którym chcesz zapisać plik PDF, a następnie dotknij białego znacznika w prawym górnym rogu

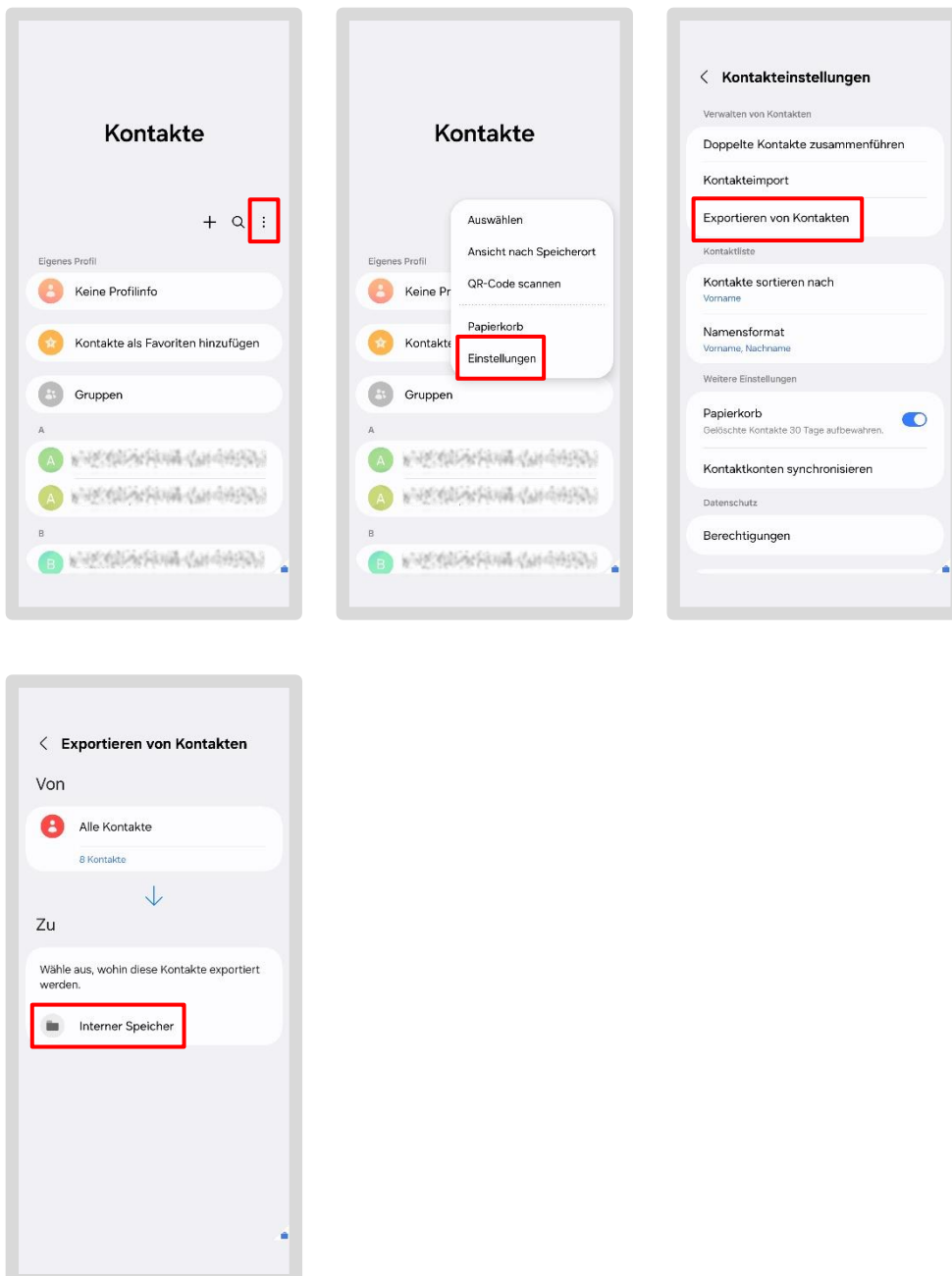


8.5 Utwórz kopię zapasową kontaktów w OneDrive

Chcesz zmienić smartfon/tablet i zabrać ze sobą kontakty?

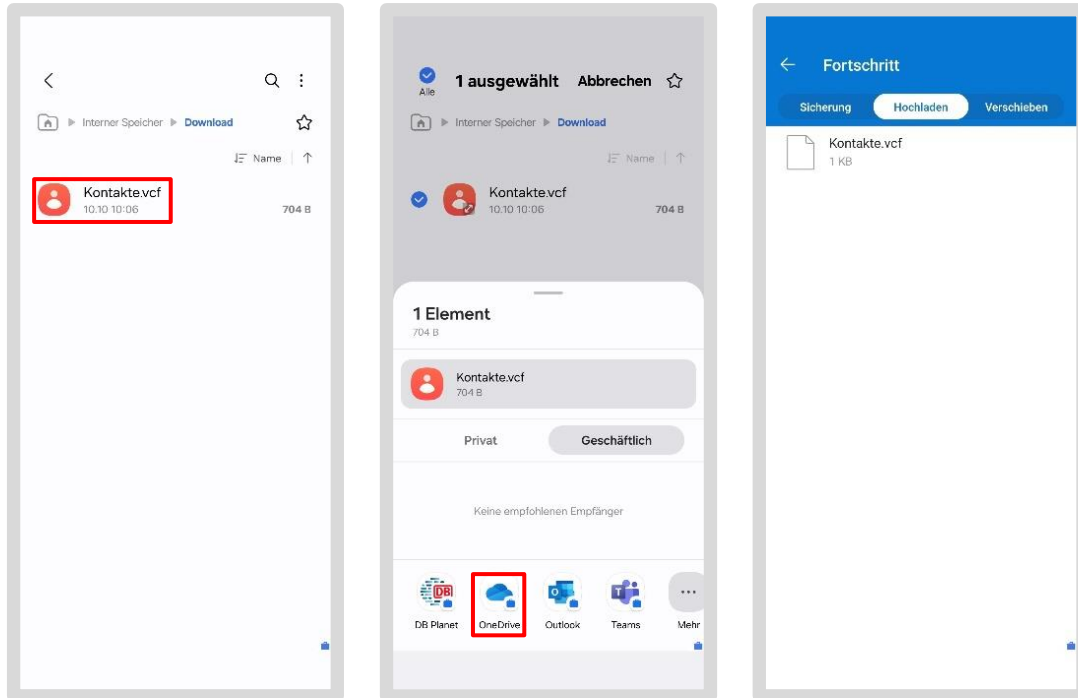
W takim razie wykonaj następujące czynności:

- Przesuń palcem w górę na ekranie głównym
- Naciśnij „Praca” w prawym górnym rogu
- Otwórz aplikację *Kontakty*
- Naciśnij „:” (menu z trzema kropkami) w prawym górnym rogu
- Wybierz „Ustawienia”
- Naciśnij „Eksport kontaktów”
- Najpierw zapisz kontakty w „Pamięci wewnętrznej”



W folderze „Pobrane” znajdziesz teraz plik .vcf o nazwie „Contacts.vcf”.

- Wybierz plik „Contacts.vcf”
- Naciśnij „OneDrive” na dole paska wyboru



Twoje kontakty znajdują się teraz w folderze OneDrive.

8.6 Importuj kontakty z OneDrive

Aby zaimportować kontakty z powrotem do aplikacji Kontakty na nowym urządzeniu,

wykonaj następujące czynności:

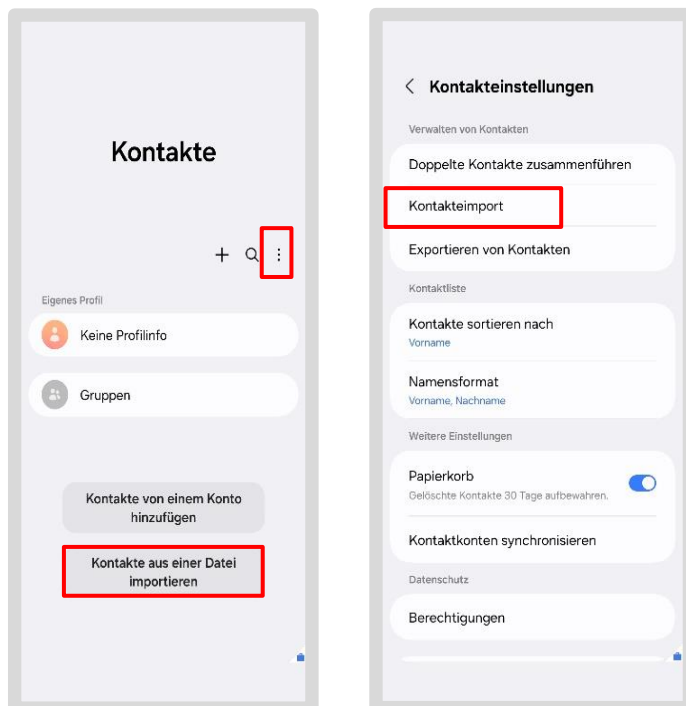
- Przesuń palcem w górę na ekranie głównym
- Naciśnij „Praca” w prawym górnym rogu
- Otwórz aplikację *Kontakty*

Jeśli **nie** masz jeszcze **żadnych nowych kontaktów**:

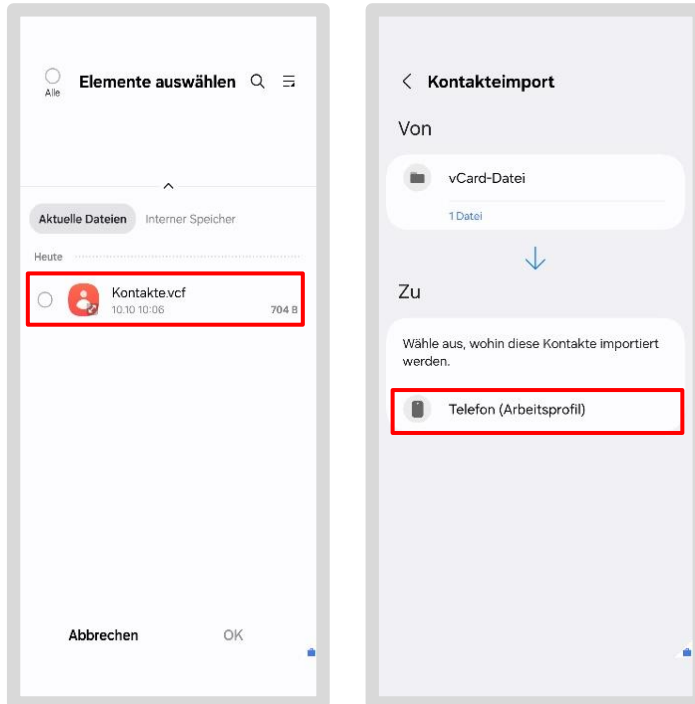
- Naciśnij „Importuj kontakty z pliku”
- Wybierz „Pamięć wewnętrzna”
- Wybierz plik „Contacts.vcf”
- Naciśnij „Telefon (profil służbowy)”
- Potwierdź, dotykając „Importuj”

Jeśli masz **już nowe kontakty**:

- Naciśnij „:” (menu z trzema kropkami) w prawym górnym rogu
- Wybierz „Ustawienia”
- Naciśnij „Importuj kontakty”
- Wybierz „Pamięć wewnętrzna”

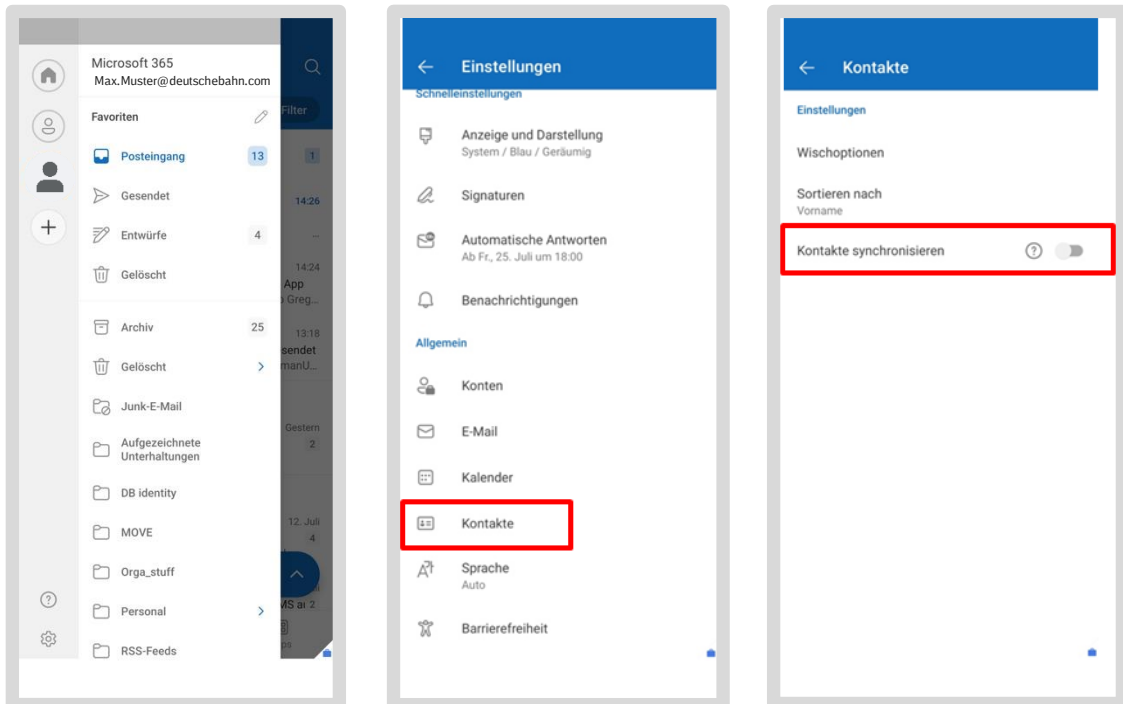


- Wybierz plik „Contacts.vcf”
- Naciśnij „Telefon (profil służbowy)”
- Potwierdź, dotykając „Importuj”



8.7 Tworzenie kopii zapasowej kontaktów za pomocą programu Outlook

- Zawsze zarządzaj kontaktami bezpośrednio w programie Outlook **na każdym urządzeniu**; w ten sposób będziesz mieć do nich dostęp ze wszystkich urządzeń i nie będziesz musiał tworzyć osobnych kopii zapasowych
- Naciśnij zdjęcie profilowe po lewej stronie słowa „Skrzynka odbiorcza”
- Naciśnij ikonę ustawień w szarym obszarze na dole, a następnie naciśnij „Kontakty” na następnym ekranie
- Włącz funkcję „Synchronizuj kontakty”, przesuważając suwak



8.8 Tworzenie kopii zapasowej haseł

Dla smartfonów/tabletów z systemem operacyjnym Android dostępna jest aplikacja „Keepass2Android”. Możesz jej używać do tworzenia kopii zapasowych i uzyskiwania dostępu do swoich haseł.

Aplikację można pobrać ze sklepu Google Play. Instrukcje dotyczące konfiguracji aplikacji można znaleźć tutaj:

> mobileworkplace.deutschebahn.com/Keepass2Android

8.9 Tworzenie kopii zapasowych danych osobowych

Jeśli na służbowym smartfonie lub tablecie przechowujesz prywatne zdjęcia, kontakty, pliki i dokumenty, musisz regularnie tworzyć ich kopie zapasowe. Dzieje się tak, ponieważ zresetowanie smartfona lub tabletu spowoduje również usunięcie danych osobowych.

Aby wykonać kopię zapasową danych osobowych, można na przykład skorzystać z **prywatnego konta Google lub prywatnego konta OneDrive**.

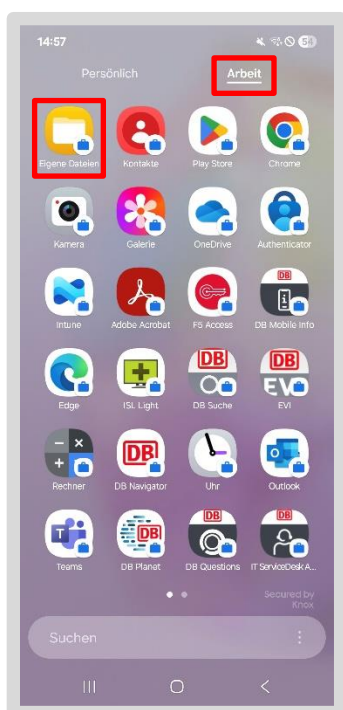
Proces tworzenia kopii zapasowej prywatnych dokumentów lub zdjęć/filmów opisano tutaj:

> mobileworkplace.deutschebahn.com/mobile-daten-sichern

8.10 Take-Off: Gdzie są Twoje zdjęcia, pliki i dokumenty?

- Twoje pliki służbowe znajdują się w sekcji „Praca/Biznes” aplikacji Moje pliki
- Aby wykonać kopię zapasową dokumentów służbowych, możesz skorzystać z aplikacji OneDrive, którą można otworzyć za pośrednictwem *aplikacji Intune*
- OneDrive poprosi o podanie służbowego adresu e-mail; wprowadź go, a Twoje konto zostanie natychmiast aktywowane! Wymaga to zainstalowania *aplikacji Outlook* i skonfigurowania konta użytkownika (adres e-mail powiązany z certyfikatem)
- Jeśli nie otrzymujesz jeszcze służbowych wiadomości e-mail lub nie skonfigurowałeś jeszcze konta e-mail dla aplikacji Outlook, zrób to tutaj.

> Zobacz [rozdział 7.3.1 Konfiguracja programu Outlook/Tworzenie konta e-mail](#)



Tworzenie kopii zapasowych dokumentów PDF lub plików Word:

- Przejdź do sekcji Dokumenty lub Pobrane
- Naciśnij i przytrzymaj plik, aż pojawi się znacznik
- Wybierz pliki, które chcesz przesłać
- Naciśnij „Wyślij”
- Wybierz „OneDrive”
- Zostaniesz przeniesiony do widoku wszystkich swoich folderów
- Wybierz folder i dotknij znacznika, aby przesłać plik
- Nie możesz znaleźć folderu? Naciśnij menu w lewym górnym rogu
- W sekcji „Biblioteki” wybierz dodatkowe foldery i dotknij ikony zaznaczenia, aby przesłać plik

Tworzenie kopii zapasowych zdjęć i filmów:

- Otwórz aplikację „OneDrive”
- Naciśnij „Zdjęcia”
- Włącz tworzenie kopii zapasowej z aparatu/aktualizację z aparatu
- W przypadku iPhone'a/iPada: Aktywuj służbową pocztę e-mail
- Następnie dotknij „Potwierdź”

Utwórz kopię zapasową danych osobistych

Aby wykonać kopię zapasową danych osobistych, możesz użyć na przykład swojego osobistego konta Google lub Apple albo osobistego konta OneDrive.

> Instrukcje wraz z sugestiami dotyczącymi tworzenia kopii zapasowej danych osobistych znajdziesz [tutaj](#)

9 Ochrona danych i informacje o użytkowaniu

Jeśli korzystasz ze smartfona/tabletu DB podczas podróży, zawsze istnieje ryzyko, że osoby nieuprawnione mogą uzyskać dostęp do urządzenia. Nawet krótki dostęp daje szansę na uzyskanie dostępu do poufnych danych.

Dlatego prosimy o przestrzeganie następujących podstawowych zasad:

1. Nie zostawiaj smartfona ani tabletu gdzie popadnie; zawsze upewnij się, że pozostaje on pod Twoją kontrolą.
2. Nie oddawaj smartfona/tabletu innym osobom, nawet „tylko na chwilę”, chyba że jest to urządzenie współdzielone.
3. Zawsze zabezpieczaj smartfon/tablet kodem PIN lub silnym hasłem, a jeszcze lepiej dodatkowymi zabezpieczeniami biometrycznymi, takimi jak odcisk palca lub rozpoznawanie twarzy.
4. Hasła i kody PIN należy używać tylko raz!
5. Hasła i kody PIN nie powinny dać się odgadnąć, dlatego nie należy używać numerów telefonów, dat urodzin, numerów rejestracyjnych samochodów ani imion.
6. Kod PIN musi mieć co najmniej sześć cyfr, zawierać co najmniej cztery różne znaki i nie może składać się z sekwencji kolejnych cyfr rosnących lub malejących.
7. Hasła muszą zawsze mieć co najmniej dwanaście znaków i zawierać co najmniej trzy z czterech następujących elementów: wielkie litery, małe litery, cyfry, znaki specjalne.
8. Nigdy nie przechowuj haseł, kodów PIN ani nazw użytkownika do smartfona/tabletu lub konta użytkownika DB na samym urządzeniu. Nawet pod postacią numeru telefonu – wszyscy znają ten trik.
9. Należy niezwłocznie i regularnie tworzyć kopie zapasowe danych służbowych i osobistych. Można to zrobić, zapisując je w usłudze OneDrive lub wysyłając je jak najszybciej pocztą elektroniczną do odpowiedniego odbiorcy. Tylko wtedy są one bezpieczne. Dzięki temu DB-IT będzie miało do nich dostęp, jeśli urządzenie użytkownika ulegnie awarii lub zostanie zgubione.

Warunki użytkowania „Mobilnej komunikacji danych”

Przyjmując smartfon/tablet i niniejsze warunki użytkowania, pracownik potwierdza zgodę na przestrzeganie warunków użytkowania:

1. Urządzenia użytkownika końcowego są osobistym sprzętem służbowym. Przekazywanie urządzenia użytkownika końcowego lub danych dostępowych/hasła/kodów PIN osobom trzecim (np. członkom rodziny lub przełożonym) jest niedozwolone.
2. Urządzenie użytkownika końcowego pozostaje własnością DB Systel przez cały okres użytkowania. Urządzenie należy zwrócić po zakończeniu okresu użytkowania. Musi ono być zawsze wolne od praw osób trzecich; w szczególności nie wolno go wypożyczać ani sprzedawać osobom trzecim.
3. Zabronione jest korzystanie, używanie i rozpowszechnianie treści oraz aplikacji o charakterze obraźliwym, zniesławiającym, pornograficznym, seksistowskim, rasistowskim, antykonstytucyjnym, niemoralnym lub przestępczym.
4. Z urządzeniem użytkownika końcowego należy obchodzić się ostrożnie i z szacunkiem. Urządzenie użytkownika końcowego można ładować wyłącznie za pomocą ładowarek i kabli dostarczonych przez producenta (w tym w zakresie dostawy). Ładowanie w godzinach pracy jest dozwolone.
5. Wszelkie utraty, kradzieże lub uszkodzenia, które ograniczają funkcjonalność, należy niezwłocznie zgłaszać bezpośrednio przełożonemu w podległości organizacyjnej.*
6. O ile jest to możliwe i pracodawca ma taką możliwość, korzystanie z danych na urządzeniu użytkownika końcowego powinno odbywać się przede wszystkim za pośrednictwem sieci Wi-Fi.
7. Ustawienia zabezpieczeń urządzenia (zasady, skaner antywirusowy, konfiguracja urządzenia itp.) nie mogą być zmieniane ani wyłączane.

¹ Zob. również załącznik 1 do Ogólnych i szczególnych warunków korzystania z usług IT KBV, p

² Zob. również Polityka ochrony aktywów DB, 136.01.03

9.1 Wyjazd: Aspekty bezpieczeństwa

Praca ze smartfonem/tabletem stanowi część Twoich obowiązków służbowych. Urządzenie to jest własnością DB Systel i dlatego należy obchodzić się z nim ostrożnie.

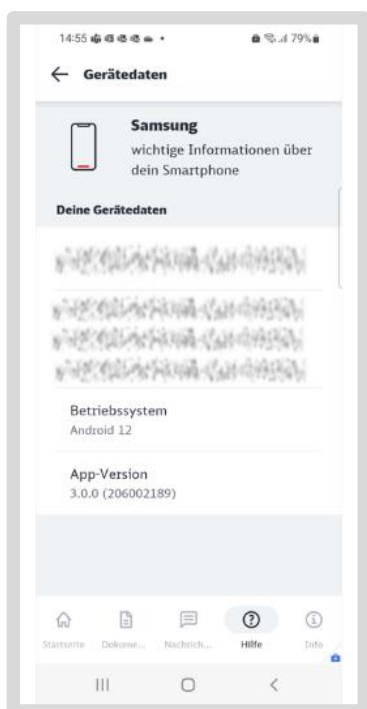
Jest to część Twojej pracy, więc nie pożyczaj go ani nie sprzedawaj.

> Jeśli smartfon/tablet musi zostać zwrócony ze względów bezpieczeństwa, prosimy o zwrot zgodnie z opisem [tutaj](#)

Nie dawaj złodziejom szansy: używaj silnego hasła. Na przykład nie przyklejaj karteczki z hasłem na ekranie.

Ochrona danych: Gdzie mogę znaleźć dane dotyczące mojego smartfona/tabletu?

W tym celu otwórz aplikację Welcome, skorzystaj z zakładek u dołu ekranu, aby przejść do zakładki „Pomoc”, a następnie wybierz podpunkt „Dane urządzenia”. Zostaną tam wyświetlone dane Twojego smartfona/tabletu, takie jak numer seryjny, IMEI lub wersja systemu operacyjnego (np. Android 13 lub iOS 17.5.1).



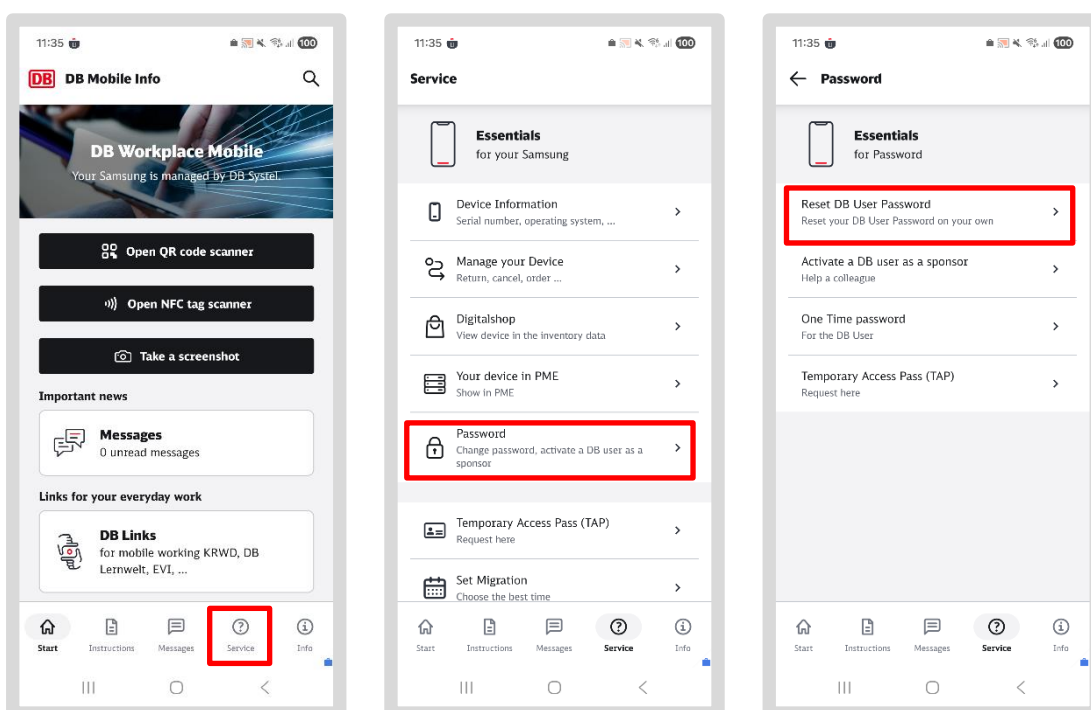
10 Zapomniałeś hasła, zwracasz urządzenie

Zapomniałeś hasła blokady ekranu lub nie pamiętasz hasła użytkownika DB? Outlook ciągle się zawiesza? Pojawiają się komunikaty o błędach, których nie rozumiesz? Nie martw się, tutaj znajdziesz pomoc.

10.1 Zapomniane lub zmiana hasła użytkownika DB

Jeśli nie pamiętasz już danych logowania do konta użytkownika DB lub chcesz je zmienić, możesz to zrobić w następujący sposób:

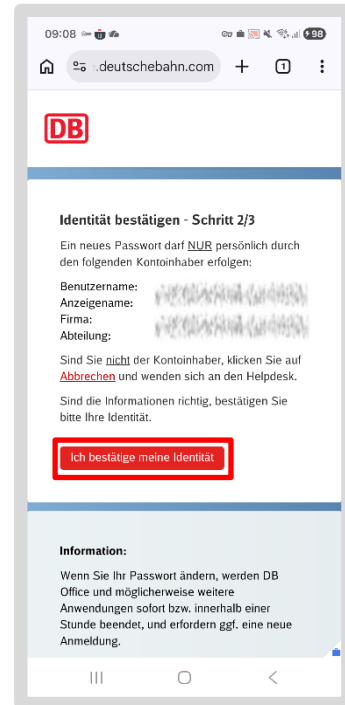
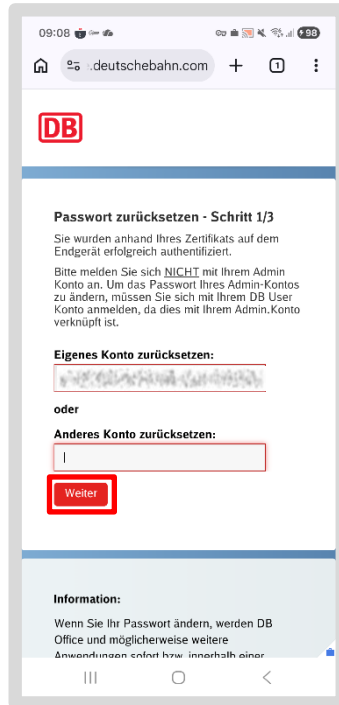
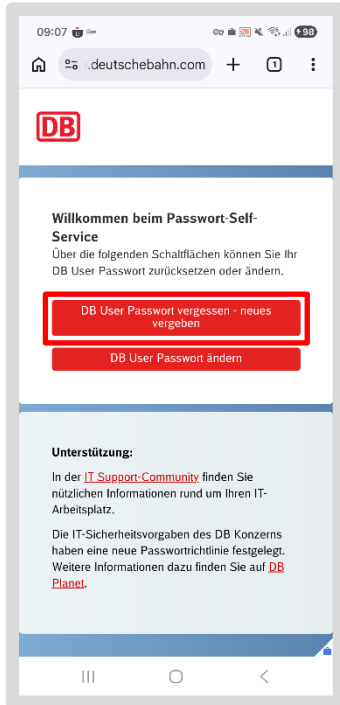
- W aplikacji **DB MOBIL** wybierz zakładkę „Serwis”
- Naciśnij „Hasła”
- Następnie dotknij „Zresetuj hasło użytkownika bazy danych”



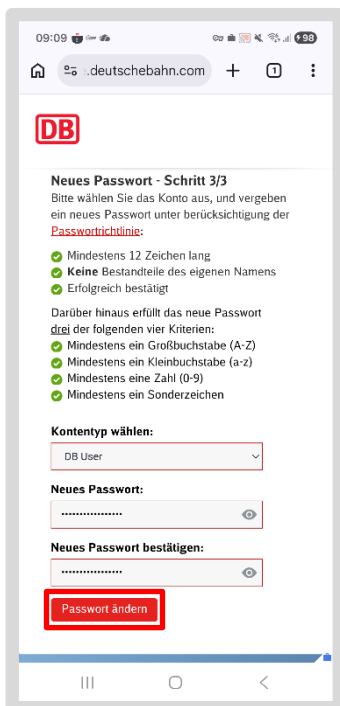
Uwaga: W tym momencie połączenie z serwisem F5 Access zostanie nawiązane automatycznie. Jest to konieczne do wykonania kolejnych czynności. Jeśli połączenie z serwisem F5 Access nie zostało nawiązane, musisz je aktywować ręcznie, aby kontynuować!

Jeśli wszystko wykonałeś poprawnie, zostaniesz teraz przekierowany na stronę samoobsługi haseł.

- Teraz wybierz przycisk, który dotyczy Ciebie
- Naciśnij „Kontynuuj” bez wpisywania niczego
- Następnie potwierdź swoją tożsamość



- Teraz wprowadź nowe hasło, uwzględniając zasady dotyczące haseł
- Potwierdź wprowadzone dane, klikając „Zmień hasło”



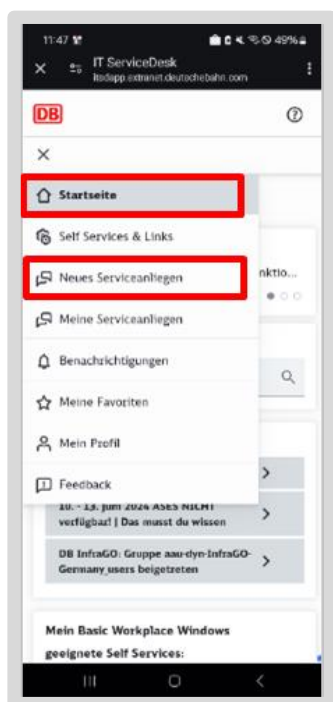
10.2 Pomoc za pośrednictwem aplikacji IT ServiceDesk



Aplikacja IT ServiceDesk stanowi centralny punkt kontaktowy w sprawach technicznych. Od analizy usterek po wsparcie techniczne w kwestiach związanych ze sprzętem i oprogramowaniem na Twoim urządzeniu – tutaj możesz zadawać pytania oraz uzyskać dostęp do pomocnych poradników i ważnych linków.

Jak uzyskać dostęp do aplikacji IT ServiceDesk

- Otwórz „aplikację IT ServiceDesk” w sekcji „Praca/Biznes”
- Lub uzyskaj do niej dostęp poprzez link: db.de/itservicedesk
- Menu znajduje się w lewym górnym rogu aplikacji
- Kliknij „Nowe zgłoszenie serwisowe”, a następnie wybierz metodę, której chcesz użyć do przesłania zgłoszenia



W aplikacji IT ServiceDesk w sekcji „Self-Service & Links” możesz również wykonać następujące czynności:

- Zaktualizować hasło użytkownika bazy danych
- Zmienić lub usunąć numer telefonu komórkowego użytkownika bazy danych

10.3 Zgubiłeś smartfon lub tablet?

Natychmiast skontaktuj się z **IT ServiceDesk**:

- IT ServiceDesk
 - Wewnętrzny: Tel. 91-5555
 - Zewnętrzny: Tel. 0361 430 8200
- Dział pomocy technicznej IT DB Cargo
 - Tel. 91 7777 (wewnętrzny)
 - Tel. 00800 327 978 35 (zewnętrzny)
- Zgłoś utratę lub kradzież

Natychmiast poinformuj swojego opiekuna klienta (telefon komórkowy):

- Zgłoś utratę lub kradzież
- Poproś o zablokowanie karty SIM! Dzięki temu nikt nie będzie mógł wykonywać połączeń na koszt firmy
- Omów z nim kolejne kroki, aby dowiedzieć się, jak otrzymać nowy smartfon/tablet

Zgłoś utratę w Digitalshop:

- Zgłoś utratę lub kradzież za pośrednictwem Digitalshop
- Otwórz sklep internetowy pod adresem <http://www.db.de/digitalshop>
- W menu głównym, w sekcji „Dane inwentaryzacyjne”, wybierz „Urządzenia mobilne”
- Wybierz swój smartfon/tablet z listy
- Kliknij opcję „Wykonaj czynność związaną z inwentaryzacją” po lewej stronie, a następnie wybierz z menu rozwijanego opcję „Kradzież urządzenia użytkownika końcowego” lub „Utrata urządzenia użytkownika końcowego”
- W razie jakichkolwiek pytań prosimy o kontakt z opiekunem umowy (telefon komórkowy)!

10.4 Uszkodzony smartfon/tablet

Natychmiast poinformuj swojego opiekuna umowy (telefon komórkowy):

- Zgłoś całkowitą utratę
- Omów z nim kolejne kroki, aby dowiedzieć się, jak otrzymać nowy smartfon/tablet

Zdeaktywuj smartfon/tablet w Digitalshop:

- Otwórz Digitalshop pod adresem <http://www.db.de/digitalshop>
- W menu głównym, w sekcji „Dane inwentaryzacyjne”, kliknij „Urządzenia mobilne”
- Wybierz swój smartfon/tablet z listy
- Naciśnij „Wykonaj czynność inwentaryzacyjną” po lewej stronie, a następnie wybierz „Urządzenie mobilne – Anulowanie” z menu rozwijanego
- Instrukcje dotyczące wymiany znajdziesz pod adresem db.de/mobile-setup
- W razie pytań prosimy o kontakt z opiekunem klienta (urządzenia mobilne)!

10.5 Zwracasz smartfon/tablet?

Jeśli smartfon/tablet jest uszkodzony, krótki przewodnik dotyczący wymiany smartfonów/tabletów znajdziesz na stronie db.de/ae w sekcji Konfiguracja/Krótkie przewodniki.

Ważne: Zrób wcześniej kopię zapasową swoich danych. Dzieje się tak, ponieważ po zwrocie smartfon/tablet zostanie całkowicie wyczyszczony przez firmę zajmującą się recyklingiem. Oznacza to, że wszystkie dane (służbowe i osobiste) zostaną utracone.

Możesz wykonać kopię zapasową danych służbowych w usłudze OneDrive. Dzięki temu dane zostaną zapisane w chmurze, co pozwoli Ci uzyskać do nich dostęp w dowolnym momencie z dowolnego urządzenia (smartfonu/tabletu/komputera). Pokażemy Ci, jak skonfigurować usługę OneDrive w [rozdziale 8.2 Konfiguracja usługi OneDrive \(OneDrive\)](#) lub na stronie mobileworkplace.deutschebahn.com/mobile-daten-sichern.

Wyloguj się ze sklepu cyfrowego na smartfonie/tablecie:

- Otwórz Sklep cyfrowy pod adresem <http://www.db.de/digitalshop>
- W menu głównym, w sekcji „Dane inwentaryzacyjne”, wybierz „Urządzenia mobilne”
- Wybierz swój smartfon/tablet z listy
- Naciśnij „Wykonaj czynność inwentaryzacyjną” po lewej stronie, a następnie wybierz „Urządzenie mobilne – anulowanie” z menu rozwijanego
- Instrukcje dotyczące wymiany urządzenia znajdziesz na stronie db.de/mobile-setup
- W razie pytań prosimy o kontakt z opiekunem umowy (urządzenia mobilne)!

Wystarczy samodzielnie zwrócić smartfon/tablet za pośrednictwem portalu IT Asset Management:

- Zaloguj się do portalu <http://www.db.de/itverwertung>
- Zamów bezpłatną przesyłkę zwrotną
- Wybierz, czy potrzebujesz tylko etykiety zwrotnej, czy chcesz również otrzymać pudełko
- Etykietę otrzymasz pocztą elektroniczną, a pudełko zostanie dostarczone pocztą na podany przez Ciebie adres

Przygotowanie smartfona/tabletu do wysyłki:

- Usuń swoje konta osobiste ze smartfona/tabletu
- Wyjmij kartę SIM i karty pamięci
- Zabezpiecz smartfon/tablet, aby nie uległ uszkodzeniu podczas transportu, i dołącz wszystkie akcesoria (zasilacz, kabel USB do ładowania itp.) do paczki zwrotnej
- Przyklej etykietę zwrotną na pudełku i zanieś je na pocztę

10.6 Gratulacje!

Pomyślnie skonfigurowałeś swój służbowy smartfon/tablet!

Aby urządzenie zawsze działało niezawodnie, pamiętaj o instalowaniu najnowszych aktualizacji!

Mamy nadzieję, że korzystanie z niego sprawi Ci przyjemność!

Więcej informacji na temat smartfona/tabletu znajdziesz w aplikacji: DB MOBIL.

> Krótki przewodnik dotyczący tworzenia kopii zapasowych danych znajdziesz na stronie mobileworkplace.deutschebahn.com/mobile-daten-sichern