

Veri Gizliliđi Beyanı

Yayıml tarihi: 17.10.2020, Uygulama sürümü 1.5'den itibaren geçerlidir (önceki sürümler şuradan temin edilebilir:

<https://www.coronawarn.app/en/privacy>)

Bu Veri Gizliliđi Beyanında, Almanya Federal Hükümetinin resmi Corona-Warn-App'ını kullandığınızda, verilerinizin nasıl işleneceğini ve hangi veri koruma haklarına sahip olduğunuzu öğreneceksiniz.

Burada aşağıdaki konular ele alınmaktadır:

1. Corona-Warn-App'ın yayımcısı kimdir?
2. Uygulamanın kullanılması isteğe bađlı mı?
3. Verileriniz işlenmesinde hangi yasal dayanaklar söz konusudur?
4. Uygulama kimleri hedefler?
5. Hangi veriler işlenir?
6. Verileriniz niçin işleniyor?
7. Sınır ötesi uyarı sistemi nasıl çalışır?
8. Uygulamanın hangi izinlere gerek duyar?
9. Verileriniz ne zaman silinir?
10. Verileriniz kime aktarılır?
11. Verileriniz AB dışındaki ülkelere aktarılacak mı?
12. Onayınızı nasıl geri alabilirsiniz?
13. Başka hangi veri koruma haklarına sahipsiniz?
14. Veri koruma görevlisi ve iletişim

Bu metnin tüm kullanıcılar için anlaşılabilir olması amacıyla, mümkün olduğunca basit ve teknik terimler içermeyen bir metin hazırladık.

1. Corona-Warn-App'ın yayımcısı kimdir?

Bu Uygulama, Almanya Federal Hükümeti için Robert Koch-Institut (Robert Koch Enstitüsü) (**RKI**) tarafından yayımlanmaktadır. RKI, ayrıca verilerinizin, veri gizliliđi kurallarına uygun olarak işlenmesinden de sorumludur.

Enfekte olduysanız ve gönüllü olarak sınır ötesi bir uyarı tetiklediğinizde, katılımcı ülkelerdeki resmi Korona uygulamalarının kullanıcılarıyla bir temas söz konusu olursa, bu kişilerin uyarılması sağlanır. Bu durumda, hem RKI, hem de sınır ötesi uyarı sistemine katılan ülkelerin yetkili sağlık kurumları, verilerin işlenmesinden müştereken sorumlu olur. Ayrıntılar için Madde 7'ye bakın.

2. Uygulamanın kullanılması isteğe bağlı mı?

Uygulamanın kullanımı isteğe bağlıdır; Uygulamayı yüklemeniz, Uygulamanın hangi işlevlerini kullanmanız ve verileri diğer kişilerle paylaşmanız noktasında yalnızca siz karar verirsiniz. Uygulamanın veri aktarımını gerektiren tüm işlevleri, öncesinde sizin açık bir şekilde onay vermenizi ister. Onay vermezseniz veya sonradan bu onayı geri alırsanız, bu durum sizin için bir sakınca doğurmaz.

3. Verileriniz işlenmesinde hangi yasal dayanaklar söz konusudur?

Verileriniz esas itibarıyla yalnızca açık bir şekilde verdiğiniz onay temelinde işlenir. Bu bağlamdaki yasal dayanak, GVKT (Genel Veri Koruma Tüzüğü) madde 6, fıkra 1, cümle 1, bent a ve sağlık verileri durumundaki yasal dayanak ise GVKT madde 9, fıkra 2, bent a'dır. Verdiğiniz onayı, istediğiniz zaman geri alabilirsiniz. Onayınız geri alma hakkı ile ilgili ayrıntılı bilgileri madde 12'de bulabilirsiniz.

4. Uygulama kimleri hedefler?

Uygulama, en az 16 yaşında olan ve Almanya'da yaşayan kişilere yönelik hazırlanmıştır.

5. Hangi veriler işlenir?

Uygulama, mümkün olduğunca az kişisel verileri işleyecek şekilde programlanmıştır. Bu, Uygulama, RKI'nin veya diğer kullanıcıların sizin kimliğinizi, adınızı, konumunuzu veya diğer kişisel bilgilerinizi öğrenmesine olanak tanıyan verileri toplamadığı anlamına gelir. Dolayısıyla Uygulama, analiz araçları üzerinden kullanıcı davranışınızın herhangi bir değerlendirmesini yapmaz.

Uygulama tarafından işlenen veriler aşağıdaki kategorilerde sınıflandırılabilir:

a. Erişim verileri

Uygulama, RKI'nin sunucu sistemiyle (bundan böyle: **sunucu sistemi**) her veri alışverişinde, sunucu sistemi erişim verileri olarak adlandırılan verileri işler. Bu işlem, Uygulamanın güncel verilere (örneğin uyarılar için) erişebilmesi veya akıllı telefonda saklanan belirli verileri sunucu sistemine aktarabilmesi için gereklidir. Erişim verileri aşağıdaki verilerden oluşmaktadır:

- IP adresi
- Erişimin tarih ve saati
- Aktarılan veri miktarı (veya paket uzunluğu)
- Veri alışverişinin başarılı olup olmadığına dair ileti

Bu erişim verileri, Uygulamanın ve sunucu sisteminin teknik açıdan işletimini sürdürmek ve güvence altına almak için işlenmektedir. Bu süreçte siz, Uygulamanın kullanıcısı olarak şahsen tanımlanmazsınız ve sizin için bir kullanıcı profili oluşturulmaz. IP adresi, kullanım işlemi bitiminden sonra saklanmaz.

Bir kullanım işlemi sırasında verilerinizin IP adresinize yetkisiz atanmasını önlemek için, Uygulama, sunucu sistemine sadece özel bir giriş sunucusu üzerinden erişir. Bunun ardından giriş sunucusu, Uygulama tarafından talep edilen veya iletilen verileri, IP adresi olmaksızın, yetkili sunucuya iletir, bu sayede IP adresi sunucu sisteminde işlenmez.

b. Maruz kalma verileri

iPhone'unuzun COVID-19 bildirim sistemini (orada "maruz kalma bildirimleri" olarak adlandırılır) veya Android akıllı telefonunuzun (orada "COVID-19 temas bildirimleri" olarak adlandırılır) etkinleştirdiğinizde, akıllı telefonunuz, Bluetooth üzerinden maruz kalma verilerini göndermeye başlar ve bu veriler yakınızdaki bulunan diğer akıllı telefonlar tarafından kaydedilir. Öte yandan, kendi akıllı telefonunuz da diğer akıllı telefonlardan maruz kalma verileri alır. Gönderilen maruz kalma verileri şunları içerir:

- Rastgele kimlik kodları (bundan böyle: **rastgele kimlik numaraları**)
- Bluetooth protokol sürümü
- Bluetooth iletim gücü, desibel miliwatt (dBm) olarak

Kaydedilen karşılaşmalardaki maruz kalma verileri, ek olarak şunları içerir:

- Karşılaşmanın günü, saati ve süresi
- Bluetooth iletim gücü, dBm cinsinden

Rastgele kimlik numaraları düzenli olarak değiştirilir. Bu yöntem, akıllı telefonunuzun bu rastgele kimlikler üzerinden tanımlanmasını önlemeye yöneliktir. Akıllı telefonunuz tarafından gönderilen kendi maruz kalma verileriniz ve temas halinde olduğunuz kişilerin kayıtlı maruz kalma verileri, akıllı telefonunuza kaydedilir ve her ikisi de 14 günlük bir sürenin ardından silinir. Aynı şekilde gönderdiğiniz maruz kalma verileriniz, diğer Uygulama kullanıcılarının akıllı telefonları tarafından kaydedildiğinde, işlenmeye başlanır.

Lütfen dikkate alın: COVID-19 bildirim sistemi, işletim sisteminizin bir işlevidir. Dolayısıyla bu sistemin sağlayıcıları ve sorumluları, Apple (iPhone'unuz varsa) ve Google'dır (Android akıllı telefonunuz varsa). Bu bağlamda verilerin işlenmesi, bu şirketlerin veri koruma yönetmeliklerine tabidir ve RKI'nin sorumluluk ve etki alanı dışındadır. İşletim sisteminizin sürümüne ve ayarlarına bağlı olarak, fiili gösterimler, kullanım adımları ve ayar seçenekleri, bu Veri Gizliliği Beyanındaki sunumdan farklı olabilirler. Söz konusu üreticiler, size daha ayrıntılı bilgi sağlamaktadır:

- Android akıllı telefonlar için bu bilgileri Google'da, cihazınızdaki "Ayarlar" > Google > COVID-19 temas bildirimleri ve "Daha fazla bilgi" bağlantısı altında bulabilirsiniz.
- Apple iPhone'ları için bu bilgiler, cihazınızdaki "Ayarlar" > "Maruz kalma bildirimleri" ve "Maruz kalma bildirimleri böyle çalışır..." bağlantısı altında bulabilirsiniz.

c. Sağlık verileri

Sağlık verileri, bir kişinin sağlığı hakkında bilgiler içeren tüm verilerdir. Bunlar, yalnızca bir kişinin eski ve güncel hastalıklarıyla ilgili bilgileri değil, aynı zamanda hastalık riski (örneğin bir kişinin Koronavirüs ile enfekte olma riski) ile ilgili bilgilerdir. Uygulama, sağlık verilerini aşağıdaki durumlarda işler:

- Bir maruz kalma fark edildiğinde
- Bir test veya bir pozitif bulgu raporu kaydederseniz
- Uygulama üzerinden çağırdığınız test sonucu pozitif ise
- Karşılaşmalarınızı, Uygulama üzerinden olası bir enfeksiyon konusunda uyarırsanız
- Olası Korona semptomların başlangıcına ilişkin beyanda bulunursanız

Ayrıntılar 6. Maddede açıklanmıştır.

6. Verileriniz niçin işleniyor?

a. ~~Risk değerlendirme~~Maruz kalma günlüğü

Uygulamanın ana işlevlerinden biri, ~~maruz kalma günlüğüdür. risk değerlendirme~~dir. Bunun görevleri, Korona testi pozitif çıkan kişilerle olası temaslar (maruz kalmalar) konusunda sizi sınır ötesi ortamda da uyarmak, enfeksiyon riskinizi hesaplamak ve size bu bağlamda gerekli davranış ve sağlık bilgileri temin etmektir.

Bu amaç için Uygulama, arka planda çalışarak sunucu sisteminden, Korona testi pozitif çıkan ve sınır ötesi uyarı sistemine katılan ülkelerin resmi Korona uygulamaları aracılığıyla gönüllü olarak bir uyarı tetikleyen kullanıcılardan rastgele kimlik numaraları ve varsa semptomların başlangıcına ilişkin bilgiyi içeren günlük bir liste çağırır (bundan böyle: **pozitif liste**). Pozitif listedeki rastgele kimlik numaraları, ek olarak ayrıca bir taşıma riski değeri ve tanı tipi hakkında bilgi de içerir (bkz. Madde 6 c.).

Uygulama bu rastgele kimlik numaralarını, COVID-19 bildirim sistemine aktarır ve bu sistem bu kodları daha önce kaydedilen rastgele kimlik numaraları ile karşılaştırır. COVID-19 bildirim sistemi bir eşleşme saptarsa, söz konusu maruz kalma için kaydedilen maruz kalma verilerini Uygulamaya aktarır. Bu veriler ve pozitif listedeki bilgiler (taşıma riski değeri, semptomların başlangıcına ilişkin bilgiler) enfeksiyon riskinizi belirlemek için Uygulama tarafından değerlendirmeye alınır. Bu verilerin hesaplanmasını belirleyen değerlendirme algoritması, RKI'nin güncel bilimsel bulgularına (örn. temas süresinin enfeksiyon riski üzerindeki etkisi) dayanmaktadır. Yeni bulgular olması durumunda RKI, Uygulamanın değerlendirme ayarları üzerinden değerlendirme algoritmasını güncelleyebilir. Bu durumda, yeni değerlendirme ayarları pozitif listeye birlikte Uygulamaya aktarılır.

Enfeksiyon riski, yalnızca Uygulama içinde hesaplanır ve COVID-19 bildirim sistemine veya diğer alıcılara (RKI, Almanya'daki diğer sağlık kurumları veya diğer ülkeler, Apple, Google ve diğer üçüncü taraflar da dahil olmak üzere) aktarılmaz.

b. Test kaydetme

Korona testi yaptırdıysanız, testinizi Uygulamaya kaydedebilirsiniz. Test sonucu hazır olur olmaz, Uygulama sizi bu konuda bilgilendirecektir. Ancak bu bilgilendirme, test laboratuvarının sunucu sistemine bağılı olmasını ve sizin ayrıca, test sonuçlarınızın test süreci kapsamında laboratuvar tarafından sunucu sistemine (test sonuçları veritabanı) aktarılmasına onay vermenizi gerektirir. Uygulamanın sunucu sistemine bağılı olmayan laboratuvarlardan gönderilen test sonuçları görüntülenemez. Bir QR kod almadıysanız, bu işlevi kullanamazsınız.

Test kaydı

Test sonucunu Uygulama aracılığıyla çağırmak için, testinizi kaydetmelisiniz. Bunun için doktorunuzdan veya testin yapıldığı tesisten bir QR kod alırsınız. Bu QR kod, Uygulama ile okunabilen bir kod numarası içerir. Bu testi kaydetmek için, bu QR kodu akıllı telefonunuzun kamerasıyla Uygulamaya taramanız gerekir. Okunan kod numarası, Uygulama tarafından karma hale getirilir. Bunun anlamı, kod numarasının spesifik bir matematik yöntemi ile sürece yabancılaştırılması ve böylece artık tanınmaz hale gelmesidir. Akıllı telefonunuz internete bağlanır bağlanmaz, Uygulama bu karma kod numarasını sunucu sistemine iletir. Bunun karşılığında Uygulama, sunucu sisteminden bir belirteç, yani bir dijital erişim kodu alır ve bu da Uygulamaya kaydedilir. Belirteç, sunucu sistemindeki karma kod numarasına bağılıdır. Uygulama daha sonra akıllı telefonunuzdaki karma kod numarasını siler. Testinizin kaydedilmesi böylece tamamlanmış olur. Her bir karma kod numarası için sunucu sistemi yalnızca bir kez bir belirteç verir. Bu sayede QR kodunuzun Uygulamanın diğer kullanıcıları tarafından test sonuçlarını sorgulamak için kullanılmasının önüne geçilir.

Test sonucunun saklanması

Test laboratuvarı test sonucunu hazırladığında, hemen bu sonucu ilgili karma kod numarası ile birlikte RKI tarafından işletilen test sonuçları veri tabanına kaydedilmek üzere gönderir. Test sonuçları veri tabanı, sunucu sistemi içinde ayrı bir sunucuda bulunur. Test laboratuvarı, Uygulamanın kullandığı matematik yönteminin aynısını kullanarak, size verilen QR kodda yer alan kod numarası bazında karma kod numarasını oluşturur.

Test sonucunun çağırılması

Uygulama, düzenli olarak belirteci kullanarak sunucu sisteminden kayıtlı testinizin durumunu sorgular. Bu bağlamda sunucu sistemi, bu belirteci karma kod numarasına atar ve bunu test sonuçları veri tabanına iletir. Veri tabanı sistemi, bu karma kod numarası için bir test sonucunun yüklenip yüklenmediğini denetler ve sonucu geriye bildirir. Sunucu sistemi, daha sonra işlemin durumunu ve test sonuçları veri tabanından sorgulanan test sonucunun kendisini (yani test sonucunuzun pozitif veya negatif çıktığını) Uygulamaya iletir. Uygulamadaki test durumu bildirimlerini etkinleştirdiyseniz (“Ayarlar” > “Bildirimler” altında), ilgili bildirim alırsınız. Uygulamayı açtığınızda, test sonucu size gösterilir.

Korona testiniz pozitif çıkmışsa, Uygulama, tekrar belirteci kullanarak sunucu sisteminden bir TAN (işlem numarası) ister. TAN, Uygulama tarafından tetiklenen bir uyarı durumunda, diğer kullanıcılara yanlış uyarı verilmesini önlemek için gerekli olur. Bu amaçla, sunucu sistemi belirteci

tekrar karma kod numarasına atar ve test sonuçları veri tabanından bu karma kod numarası için gerçekten bir pozitif test sonucunun mevcudiyetini doğrulamasını ister. İlgili doğrulama alındığında, sunucu sistemi TAN'ı oluşturur ve bunu uygulamaya iletir. Bu TAN'ın bir kopyası sunucu sisteminde kalır.

c. Diğer insanların uyarılması

Korona testiniz pozitif çıkmışsa, bu Uygulamayı veya katılımcı ülkelerin resmi Korona uygulamalarını kullanan diğer kullanıcıları uarmak için sınır ötesi uyarı işlevini kullanabilirsiniz. Bu durumda, Uygulama şu verileri sunucu sistemine iletir:

- Son 14 gündeki kendi rastgele kimlik numaralarınız
- Semptomların başlangıcına ilişkin olası bilgi
- TAN'ınız (bkz. Madde 6 b.)

Akıllı telefonunuz, ilk önce COVID-19 bildirim sisteminden kendi rastgele kimlik numaralarınızı Uygulamaya aktarmak için sizden izin isteyebilir.

Rastgele kimlik numaraları sunucu sistemine iletilmeden önce, Uygulama rastgele kimlik numaralarına ayrıca bir taşıma riski değeri ve tanı tipi hakkında verileri ekler (bunun için Madde 6 a'ya bakın). Uygulamanın uyarı işlevi, sadece laboratuvarında onaylanan tanıları kullanılabilirdiğinden, tanı tipi tüm kullanıcılar için aynıdır. Taşıma riski değeri, ilgili rastgele kimlik numarasının kullanıldığı gündeki enfeksiyon olasılığının bir tahmini değeridir. Enfeksiyon olasılığı, enfeksiyonun süresine ve seyrine bağlı olduğundan, örneğin bir maruz kalma gününde, semptomların başlangıcından bu yana ne kadar zaman geçmişse, o gün enfeksiyon riski o kadar düşük olur.

Sorgulanan semptomların başlangıcına ilişkin bilginin verilmesi, isteğe bağlıdır. Ancak bu bilgi, taşıma riski değerinin daha kesin bir şekilde hesaplanmasında yardımcı olmaktadır. Bu bilgiyi sağlamadığınızda, enfeksiyonun tipik seyri varsayılarak taşıma riski değeri hesaplanır, yani rastgele kimlik numarası kullanımından sonra geçen süre ne kadar uzunsa, ilgili taşıma riski değeri o kadar küçük olur.

Uygulama üzerinden test sonucunuzu almadıysanız:

Pozitif test sonucunuzu Uygulama üzerinden çağırmanız olsanız bile, diğer insanları uyarabilirsiniz. Bunun için, "TAN iste" prosedürünü seçin. Bunun üzerine Uygulama sizden yardım hattını aramanızı ister. Orada bir yardım hattı çalışanı, Korona testinizin pozitif çıktığından emin olmak için size birkaç soru soracaktır. Bunun amacı, yanlış uyarıların istemeden veya kasıtlı olarak tetiklenmesini önlemektir. Bu soruları doğru yanıtladıktan sonra, size cep telefonu / telefon numaranız ve adınız sorulacaktır. Bu, daha sonra sizi telefonla arayarak, Uygulamaya girmeniz gereken ve TeleTAN olarak adlandırılan kodu size bildirmek içindir. Cep telefonunuz / telefon numaranız ve adınız, yalnızca bu süreçte geçici olarak kaydedilecek ve en geç bir saat içinde silinecektir. Aramanızdan hemen sonra, yardım hattı çalışanı, sunucu sistemindeki özel bir erişim yolu üzerinden TeleTAN'ınızı oluşturacak ve bu konuda bilgi vermek için sizi arayacaktır. Bir TeleTAN yalnızca bir saat süreyle geçerli kalır ve dolayısıyla size iletdikten hemen sonra, ancak en geç bir saat içinde yardım hattındaki sistemden silinir. Uygulamaya geçerli bir TeleTAN girildikten sonra, bu kod doğrulama için sunucu sistemine iletilir. Doğrulama başarılı olursa

Uygulama, sunucu sisteminden bir belirteç, yani bir dijital erişim kodu alır ve bu da Uygulamaya kaydedilir. Uygulama daha sonra bu belirteci sunucu sisteminden bir TAN talep etmek için kullanır.

d. Uygulamanın bilgilendirme amaçlı kullanımı

Uygulamayı yalnızca bilgi edinme amaçlı kullanıyorsanız, yani yukarıda belirtilen işlevlerden hiçbirini kullanmıyorsanız, veri işleme yalnızca kendi akıllı telefonunuzda gerçekleşir ve RKI tarafından hiçbir kişisel veri işlenmez. Uygulamada, örneğin www.bundesregierung.de gibi bağlantılı web siteleri açılır ve standart tarayıcıda (Android akıllı telefonlar) veya Uygulamada (iPhone'lar) görüntülenir. Hangi verilerin işleneceği, erişilen web sitesinin ilgili sağlayıcısı tarafından belirlenmektedir.

7. Sınır ötesi uyarı sistemi nasıl çalışır?

Diğer ülkelerdeki resmi Korona uygulamalarının kullanıcılarının da uyarılmasını için RKI, bu ülkelerdeki sorumlu merciler ve kurumlar (bundan böyle: **sağlık kurumları**) ile birlikte uyarı mesajlarının sınır ötesi değişimine yönelik merkezi bir uyarı sunucusu (bundan böyle: **veri değişim sunucusu**) kurmuştur. Veri değişim sunucusu, elektronik sağlık hizmetleri için üye devletler arasında kurulmuş olan ağın dijital altyapısını kullanır.

Veri değişim sunucusuna bağlı Korona uygulamalarının ulusal sunucu sistemleri, kendi pozitif listelerini düzenli olarak veri değişim sunucusuna iletir ve ondan diğer ülkelerin pozitif listelerini alır.

Sunucu sistemi, aldığı pozitif listeleri kendi pozitif listesiyle birleştirir, bu sayede **risk değerlendirilmesinde maruz kalma günlüğünde**, diğer Korona uygulamalarının kullanıcılarıyla olan riskli karşılaşmalar da dikkate alınabilir (bkz. Madde 6 c.). Diğer katılımcı ülkeler, RKI tarafından sağlanan pozitif listelerle aynı yöntemi kullanarak çalışmaktadır.

Ortaklaşa işlenen veri değişim sunucusuna, yalnızca ulusal Korona uygulamalarının uyumlu olduğu ve aynı yüksek düzeyde veri gizliliği güvencesi veren ülkelerin katılmasına izin verilmektedir. Bunun için, özellikle, katılımcı ülkelerin Korona uygulamalarının da COVID-19 bildirim sistemini kullanması, ilgili ulusal sağlık kurumları tarafından onaylanmış olması ve ayrıca kullanıcılarının gizliliğinin korunması zorunludur. İşbirliğinin teknik ve organizasyonel ayrıntıları AB Komisyonunun bir kararında belirlenmiştir (15 Temmuz 2020 tarihli Uygulama Kararı (AB) 2020/1023, bu kararı şu adresten erişebilirsiniz: https://eur-lex.europa.eu/eli/dec_impl/2020/1023/oj).

RKI ve katılımcı ülkelerin yetkili sağlık kurumları, sınır ötesi **maruz kalma günlüğü risk değerlendirilmesi** ve uyarısı sağlamak üzere veri değişim sunucusunda bulunan pozitif listelerde yer alan verilerin (rastgele kimlik numaraları ve semptomların başlangıcına ilişkin olası bilgiler) işlenmesinden müştereken sorumludur.

Sisteme katılımcı ülkeler listesinin değişebileceğini, lütfen göz önünde bulundurun. Sorumlu sağlık kurumları hakkında bilgilerin bulunduğu güncel listenin yer aldığı sıkça sorulan sorulara https://www.coronawarn.app/en/faq/#interoperability_countries adresinde erişebilirsiniz.

8. Uygulamanın hangi izinlere gerek duyar?

Uygulama, akıllı telefonunuzdaki çeşitli işlevlere ve arabirimlere erişim gerektirir. Bunun için, Uygulamaya belli bazı izinleri vermenizi gereklidir. Bu yetkilendirme sistemi, işletim sisteminizin teknik özelliklerine göre değişmektedir. Örneğin yetkilendirmeler, akıllı telefonunuzda yetkilendirme kategorilerinde birleştirilmiş olabilir ve sizin yetkilendirme kategorisini bir bütün olarak kabul etmeniz gerekebilir. Uygulama tarafından talep edilen yetkiler verilmezse, hiçbir Uygulama işlevinin kullanılamayacağını veya yalnızca birkaçının kullanılabileceğini lütfen unutmayın.

a. Teknik gereksinimler (tüm akıllı telefonlar)

- Uygulama, sunucu sistemiyle veri alışverişinde bulunabilmek için internet bağlantısı gerektirir.
- Akıllı telefonunuzun kendi rastgele kimlik numaralarını gönderebilmesi ve diğer akıllı telefonlardan rastgele kimlik numaralarını kaydedebilmesi için, Bluetooth işlevinin etkinleştirilmesi zorunludur.
- Uygulama, enfeksiyon riskinizi otomatik olarak belirlemek ve bir kayıtlı testin durumunu sorgulamak için akıllı telefonunuzda arka planda çalışabilmelidir. Arka plan işletimini devre dışı bırakırsanız, Uygulamanın tüm eylemlerini kendiniz başlatmanız gerekir.

b. Android akıllı telefonları

Bir Android akıllı telefon kullanıyorsanız, ayrıca aşağıdaki sistem işlevlerinin de etkinleştirilmesi gerekir:

- Android'in COVID-19 bildirim sistemi (COVID-19 temas bildirimleri)
- Sürüm 10'a kadar olan Android sürümlerinde konum belirleme özelliği etkinleştirilmelidir. Ancak konum verileri toplanmaz.
- Enfeksiyon riskinizin ve test sonuçlarının durumlarındaki değişikliklerden haberdar olmak için, bildirim işlevinin etkinleştirilmiş olmalıdır. Bildirim işlevi, işletim sisteminde standart olarak etkinleştirilmiştir.

Bunların yanı sıra Uygulama aşağıdaki yetkilere gerek duyar:

- "Testi kaydet" işlevi, QR kodu okuyabilmek için kameraya erişim yetkisi gerektirir.

c. iPhone'lar (Apple iOS)

Bir iPhone kullanıyorsanız, aşağıdaki sistem işlevlerinin de etkinleştirilmesi gerekir:

- iOS'in COVID-19 bildirim sistemi (maruz kalma bildirimleri)
- Enfeksiyon riskinizin ve test sonuçlarının durumlarındaki değişikliklerden haberdar olmak için, bildirimler işlevi etkinleştirilmiş olmalıdır.

Bunlara ek olarak Uygulama aşağıdaki yetkilere gerek duyar:

- "Testi kaydet" işlevi, QR kodu okuyabilmek için kameraya erişim yetkisi gerektirir.

9. Verileriniz ne zaman silinir?

Saklama süresi, verilerinizin kaydedildiği amaçlara veya Uygulama işlevlerine göre değişmektedir. Verilerin saklama süresini belirlerken RKI, inkübasyon dönemi (14 güne kadar) ve enfekte bir kişinin inkübasyon dönemi bitiminden sonra diğer insanlar için oluşturduğu enfeksiyon riskinin süresine ilişkin güncel bilimsel bulguları dikkate alır. Madde 6'da daha kısa bir saklama süresi belirtilmedikçe, aşağıdaki süreler geçerlidir:

a. Akıllı telefonunuzdaki veriler

Çağrılan pozitif listeler 14 gün sonra Uygulama belleğinden silinir. Uygulamada hesaplanan enfeksiyon riski (örn. "düşük risk"), her güncellemeden sonra, ancak en geç 14 gün sonra Uygulama belleğinden silinir. Pozitif Korona testi kaydettiyseniz, bir uyarı tetikledikten hemen sonra belirteç, Uygulama belleğinden silinir.

b. Sunucu sistemlerindeki veriler

Pozitif listeler, 14 gün sonra tüm sunucu sistemlerinden (değişim sunucuları dahil) silinir. Diğer tüm veriler en geç 21 gün sonra silinir.

10. Verileriniz kime aktarılır?

Uygulama aracılığıyla diğer kullanıcıları uyardığınızda, son 14 güne ait rastgele kimlik numaralarınız ve semptomların başlangıcına ilişkin isteğe bağlı bilgiler, veri değişim sunucusuna katılan ülkelerin sorumlu sağlık kurumlarına gönderilir ve oradan da sınır ötesi uyarı sistemine katılan resmi Korona uygulamalarının sunucu sistemlerine aktarılır. Ulusal Korona uygulamalarının sunucu sistemleri, verilerinizi pozitif listelerin bir ögesi olarak kendi kullanıcılarına dağıtır.

Katılımcı ülkelerin yetkili ulusal sağlık kurumları, ortaklaşa işletilen uyarı sisteminin işletimi ve bakımı için AB Komisyonunu işletici kuruluş olarak görevlendirmiştir.

RKI, Uygulamanın teknik altyapısının bir bölümünün (örn. sunucu sistemleri, yardım hattı) işletimi ve bakımı için, işletici kuruluş olarak T-Systems International GmbH ve SAP Deutschland SE & Co. KG firmalarını görevlendirmiştir. Bu firmalar, aynı zamanda AB Komisyonu tarafından, katılımcı ülkelerin ortaklaşa işletilen uyarı sisteminin teknik yapısının temini ve idaresi için alt işleyici olarak görevlendirilmektedir.

Sözü gelmişken, RKI, Uygulamanın kullanımıyla bağlantılı olarak toplanan verilerinizi, yalnızca RKI'nin yasalar tarafından yükümlü kılınması veya Uygulamanın teknik altyapısına bir saldırı olması durumunda bir yasal takibat veya cezai kovuşturma için ifşa edilmesi gerekli olduğu takdirde üçüncü taraflara aktarır. Diğer durumlarda veri aktarımı gerçekleşmez.

11. Verileriniz AB dışındaki ülkelere aktarılacak mı?

Bir uyarı tetiklediğinizde, ortaklaşa işletilen veri değişim sunucusuna bağlı Korona uygulamaları dünya çapındaki mevcut pozitif listeleri çağırabilir, böylece tatilde veya iş gezisinde olan kullanıcılar da uyarılabilir. Ancak Uygulama tarafından aktarılan veriler, sadece Almanya'daki sunucularda veya bir diğer AB (veya Avrupa Ekonomik Alanı) ülkesindeki sunucularda işlenir, dolayısıyla Genel Veri Koruma Tüzüğü'nün (GVKT) katı gerekliliklerine tabidir.

12. Onayınızı nasıl geri alabilirsiniz?

Geleceğe dönük geçerli olmak üzere, Uygulamada RKI'ye verdiğiniz onayı istediğiniz zaman geri alma hakkına sahipsiniz. Ancak bu, iptal işlemi geçerli oluncaya kadar bu onay temelinde yürütülmüş olan işlemlerin yasalara uygunluğunu etkilemez.

a. ~~Risk değerlendirme~~ Maruz kalma günlüğü onayı

Onayınızı geri almak için, ~~risk değerlendirme~~ maruz kalma günlüğünü devre dışı bırakabilir veya Uygulamayı silebilirsiniz. ~~Risk değerlendirme~~ Maruz kalma günlüğünü tekrar kullanmak isterseniz, kaydırıcıyı yeniden etkinleştirebilir veya uygulamayı yeniden yükleyebilirsiniz.

b. Test kaydı için onay

Onayınızı geri almak için, test kaydetmeyi devre dışı bırakabilir veya Uygulamayı silebilirsiniz. Bunun ardından test sonucunu çağırma için kullanılan belirteç, Uygulama belleğinden silinir, böylece belirteç artık sunucu sisteminde atanamaz. Bu durumda aynı testi tekrar kaydetmeniz artık mümkün olmaz. Yeni bir test kaydetmek isterseniz, sizden yeniden onay vermeniz istenecektir.

c. Uyarı işlevi onayı

Onayınızı geri almak için, Uygulamayı silmeniz gerekmektedir. Sunucu sistemine halen iletilmiş olan rastgele kimlikleriniz, Uygulama belleğinden silinecek ve artık atanamayacaktır. Daha sonra tekrar bir uyarı tetiklemek isterseniz, Uygulamayı yeniden yüklemeniz ve tekrar onay vermeniz gerekir. Uygulamaya kaydedilmiş olan test sonucu, başkalarını uyarmak için tekrar kullanılamaz.

RKI, rastgele kimliklerinizi ve taşıma riski değerlerinizi, sunucu sistemi tarafından dağıtılmış olan pozitif listelerden ve kullanıcıların akıllı telefonlarından silme olanağına sahip değildir. Ayrıca COVID-19 bildirim sisteminde saklanan maruz kalma verilerinizi silme işlemi, muhtemelen akıllı telefonunuzun sistem ayarlarında manuel olarak gerçekleştirmelisiniz. Bunun için ayrıca Madde 5 b altındaki bilgileri dikkate alın.

13. Başka hangi veri koruma haklarına sahipsiniz?

Kişisel verilerinizi RKI tarafından işlendiği sürece, ek olarak aşağıdaki veri koruma haklarına da sahipsiniz:

- GVKT Madde 15, 16, 17, 18, 20 ve 21 kapsamındaki haklar,

- [RKI'nin veri koruma görevlisi](#) ile iletişim geçme ve isteklerinizi dile getirme hakkı (GVKT Madde 38 fıkra 4 uyarınca) ve
- yetkili veri koruma denetim makamına şikayette bulunma hakkı. Bunun için ya ikâmet yerinizdeki yetkili denetim makamı ya da RKI için yetkili makam ile iletişime geçebilirsiniz. RKI için yetkili denetim makamı: Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Federal Veri Koruma ve Bilgi Özgürlüğü Komiseri) Graurheindorfer Str. 153, 53117 Bonn.

Bu veri koruma hakları, ortaklaşa işletilen sınır ötesi veri değişim sunucusu ile ilgili olarak, veri değişim sunucusuna katılan ülkelerdeki veri işlemeden sorumlu sağlık kurumları tarafından da size tanınmaktadır (Bkz. Madde 7).

Lütfen yukarıda sözü geçen veri koruma haklarının, yalnızca bu talep edilen hakların ilgili olduğu verilerin açıkça sizin şahsınıza atanabilmesi halinde ifa edilebileceğini göz önünde bulundurun. Bu yalnızca, sunucu sistemine aktarılan verilerin, şahsınıza veya akıllı telefonunuza açık bir şekilde atanmasını sağlayan Uygulama üzerinden daha fazla kişisel verilerin toplanmasıyla mümkün olabilmektedir. Bu işlem Uygulamanın amaçları doğrultusunda gerekli olmadığından, RKI bu tür ek verileri toplamak zorunda değildir (GVKT Madde 11, fıkra 2). Kaldı ki, bu işlem, mümkün olduğunca az veri toplama hedefine ters düşecektir. Bu nedenle, yukarıda belirtilen veri koruma hakları, kimliğiniz hakkında vermiş olduğunuz ek bilgilerle bile genellikle yerine getirilememektedir.

14. Veri koruma görevlisi ve iletişim

Veri gizliliğine ilişkin sorularınızı ve endişelerinizi RKI'nin resmi veri koruma görevlisine gönderebilirsiniz: Robert Koch-Institut, z. H. des Datenschutzbeauftragten (veri koruma görevlisi), Nordufer 20,13353 Berlin veya e-posta yoluyla: datenschutz@rki.de.

Yayın tarihi: 17.10.2020