Yayım tarihi: 24.03.2021, Uygulama sürümü 1.1.5'ten itibaren geçerlidir (önceki sürümler şuradan temin edilebilir: https://www.coronawarn.app/de/privacy)

Veri Gizliliği Beyanı

Bu Veri Gizliliği 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:

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 kişisel verilerinizin, veri gizliliği kurallarına uygun olarak işlenmesinden de sorumludur.

Korona testiniz pozitif çıkmışsa ve sınır ötesi bir uyarı tetiklediğinizde, katılımcı ülkelerdeki resmi Korona uygulamalarının kullanıcılarıyla bir karşılaşma 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 kullanılması isteğe bağlıdır. Uygulamayı yüklemeniz, Uygulamanın hangi işlevlerini kullanmanız ve verileri diğer kişilerle paylaşmanız noktasında yalnızca siz karar

verirsiniz. Maruz kalma veya sağlık verilerinizin aktarılmasını gerektiren Uygulamanın tüm işlevleri, sizden önceden açıkça rızanızı vermenizi gerektirir. Rızanızı vermezseniz veya sonradan bu rızayı geri alırsanız, bu durum sizin için bir sakınca doğurmaz.

3. Verileriniz işlenmesinde hangi yasal dayanaklar söz konusudur?

Esas itibariyle yalnızca siz daha önce açık bir şekilde rıza beyanında bulunmuşsanız, verileriniz ancak o zaman RKI tarafından işlenir. Buradaki 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. Daha önce vermiş olduğunuz rızanızı, istediği zaman geri alabilirsiniz (geri alma hakkı). Onayınız geri alma hakkı ile ilgili ayrıntılı bilgileri Madde 12'de bulabilirsiniz. Günlük istatistiklerin alınması için erişim verilerinin işlenmesi (bkz. Madde 6 d.), GVKT madde 6, fıkra 1, bent e ile bağlantılı olarak BGA-NachfG (Federal Sağlık Kurumu Halef Kuruluşları hakkında Kanun) madde 4, fıkra 4 uyarınca RKI tarafından toplumun bilgilendirilmesi kapsamında gerçekleşir.

4. Uygulama kimleri hedefler?

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

5. Hangi veriler işlenir?

Uygulamanın tüm sistemi, mümkün olduğunca az kişisel verileri işleyecek şekilde programlanmıştır. Bu demektir ki sistem, risk değerlendirmesi, diğer kişilerin uyarılması ve test sonucunun alınması için, RKI'nin veya diğer kullanıcıların sizin kimliğinizi, adınızı, konumunuzu veya diğer kişisel bilgilerinizi öğrenmesine olanak tanıyan verileri toplamamaktadır.

Dolayısıyla Uygulama, prensip olarak analiz araçları üzerinden kullanıcı davranışınızın herhangi bir değerlendirmesini yapmaz. Sadece isteğe bağlı veri bağışına açıkça onay vermeniz durumunda, Uygulama kullanımınıza ilişkin belirli veriler, RKI'ye aktarılacaktır (bkz. Madde 5 e.).

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 yakınınızda 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
- Uygulama üzerinden bir test sonucu çağırırsanız
- Karşılaşmalarınızı, Uygulama üzerinden olası bir enfeksiyon konusunda uyarırsanız

- Olası Korona semptomların başlangıcına ilişkin beyanda bulunursanız

Ayrıntılar 6. Maddede açıklanmıştır.

d. Temas günlüğündeki veriler

Temas günlüğünüze, hangi kişilerle ne zaman ve nerede karşılaştığınızı not ederseniz, bu bilgiler akıllı telefonunuzda şifrelenmiş halde saklanır. Temas günlüğü kayıtları, yalnızca hatırlatma işlevi görür. RKI veya diğer kurumlar, temas günlüğündeki kayıtlara erişemez. Temas günlüğü, son 14 gün içindeki kişisel temaslarınızı takip etmenize yardımcı olabilir. Korona testiniz pozitif çıkarsa ve sağlık kurumu sizden temas takibinde yardım etmenizi rica ederse, sağlık kurumuna gerekli bilgileri hızlı bir şekilde aktarabilirsiniz.

Temas günlüğünün kullanılması isteğe bağlıdır. Veri girişlerinin temas günlüğüne nasıl kaydedileceğine siz karar verirsiniz. Bu açıdan veri girişlerinizden de siz sorumlusunuz. Dolayısıyla temas günlüğünüze eklediğiniz kişilerin mahremiyetine lütfen saygı gösterin. Bu bilgiler, üçüncü taraflara aktarılmamalı ve güvenli olmayan iletişim kanalları üzerinden aktarımı yapılmamalıdır. Yetkili sağlık kurumu, temas bağlantılarınızı takip etmek isterse, sizden hangi bilgilere gerek duyduğunu ve sizin bunları nasıl sağlayacağınızı size söyleyecektir.

e. Kullanım verileri (veri bağışı)

Veri bağışını etkinleştirdiğinizde Uygulama, Uygulama kullanımınıza ilişkin belirli verileri günde bir kez RKI'ye aktarır (bundan böyle: **Kullanım verileri**). Bu kullanım verileri, Uygulama tarafından görüntülenen riskli karşılaşmalar, alınan ve tetiklenen uyarılar, alınan test sonuçları ve akıllı telefonunuzun işletim sistemine ilişkin verilerdir.

Kullanım verileri ayrıntılarıyla şunlardır:

- Veri bağışının tarihi (yani aktarımın günü)
- Uyarı geçmişindeki önceki güne göre değişiklikler.
- Veri bağışı sırasında hangi risk durumunun görüntülendiği.
- Karşılaşmaların risk durumlarının hesaplama temeline ilişkin veriler.
- Akıllı telefonunuzun modeli ve sürümü ile Uygulamanızın sürümü ve kullanılan işletim sistemine ilişkin bilgiler.

Uygulama üzerinden test sonucunuzu aldıysanız:

- Test sonucunun pozitif mi yoksa negatif mi olduğu.
- Test kaydı sırasında hangi riskin görüntülendiği.
- Son riskli karşılaşmadan ve bunun Uygulamada görüntülenmesinden test kaydına kadar geçen süre.
- Bir uyarıyı tetiklemek için işlevi başlatıp başlatmadığınız ve başlattıysanız, bu süreçte hangi adıma kadar geldiğiniz (örn. semptom sorgusuna kadar gelmeniz).

Bir uyarı tetiklediyseniz:

- Semptomların başlangıcı hakkında bilgi verip vermediğiniz.
- Başkalarını uyarmak için ne zaman rıza verdiğiniz (test kaydından önce veya sonra).

- Uyarı sürecinin tamamını geçip geçmediğiniz veya uyarı işlemini daha önce yarıda bırakılıp bırakmadığınız (örneğin verilerinizin başarıyla aktarıldığına ilişkin onayı bekleyip beklemediğiniz gibi).

- Test kaydınız ile test sonucunuza erişiminiz arasında kaç saat geçtiğine ilişkin bilgi.
- Yüksek risk bildiriminden uyarının tetiklenmesine kadar geçen gün sayısı.
- Test kaydından sonra geçen saat sayısı.

Ayrıca kullanım verileriyle birlikte RKI'ye aktarılmak üzere bölgeniz ve yaş grubunuza ilişkin diğer opsiyonel verileri de sağlayabilirsiniz.

RKI, Uygulamanın etki gücünü ve işlevselliğini değerlendirmek ve pandemi hakkında yeni çıkarımlar elde etmek için, kullanım verilerini olası opsiyonel veriler ile birleştirecek ve anonimleştirilmiş istatistikler olarak değerlendirecektir.

Veri bağışına katılım, gönüllü olarak gerçekleşmektedir. Veri bağışının etkinleştirilmesi, Uygulamanızın orijinalliğinin doğrulanmasını gerektirir (bu konuyla ilgili daha fazla bilgi için bkz. Madde 5 h. ve 11.).

f. Hata raporlarının içerikleri

Hata analizi ile ilgili olarak Uygulama teknik desteğine yardımcı olmak için Uygulamanızda hata raporu kaydedebilirsiniz. Hata raporunu kaydetmeye başladığınızda,

- Uygulamadaki kullanım adımlarınız,
- teknik adımlar ve süreçler ile durum raporları
    - risk değerlendirmesi (örneğin, maruz kalma verilerinin nasıl işlendiği, enfeksiyon riskinin hesaplanması, pozitif listelerin güncellenmesi, hesaplanan risk durumunun görüntülenmesi),
    - test sonuçlarını çağrılması ve görüntülenmesi ve
    - başkalarını uyarmak için olası prosedürler (örneğin akıllı telefonunuz tarafından taşıma riski değerlerinin hesaplanması ve rastgele kimlik numaralarınızın tekniksel açıdan sağlanması)

akıllı telefonunuzda kapsamlı bir şekilde kaydedilir ve saklanır. Bir hata raporu sağlık verileri de içerebilir, çünkü bir riskli karşılaşmanın saptanmasına yönelik teknik adımlar ve süreçler de kaydedilmektedir.

Ancak hata raporu, test kaydı QR kodlarını, Uygulamanızda depolanan belirteç ve temas günlüğünüzdeki veri girişlerine ilişkin herhangi bir bilgi içermez. Hata raporu, adınızı ve RKI tarafından kimliğinizin tanımlanmasını sağlayacak diğer verileri içermez.

İstediğiniz zaman hata raporunu kaydını durdurabilir ve hata raporunu silebilirsiniz. Hata raporunu RKI ile paylaşmaya karar verdiğinizde, size Uygulama üzerinden hata raporu bir kimlik kodu (hata raporu kimlik numarası) gönderilir. Hata raporu kimlik numarası üzerinden RKI, hata raporunuzu, teknik desteğe örneğin hatanın bir açıklamasını e-posta ile ilettiğinizde ayrı olarak sağladığınız diğer bilgilere atayabilir. Hata raporu kimlik numaranızı teknik desteğe aktardığınızda, onların diğer bazı veriler aracılığıyla sizin kimliğinize bağlantı kurması mümkün olabilir.

Bir hata raporunun oluşturulması ve RKI'ye gönderimi isteğe bağlı gerçekleşir. Bir hata raporu kaydetmek ve bunu Uygulama teknik desteğe göndermek isteyip istemediğinize siz kendiniz

karar verirsiniz. Veri bağışının gönderiminin etkinleştirilmesi, Uygulamanızın orijinalliğinin doğrulanmasını gerektirir (bu konuyla ilgili daha fazla bilgi için bkz. Madde 5 h. ve 11.).

g. Ankete katılım

Uygulamada bazı kullanıcılara bir RKI anketine katılma olanağı verilir. Ankete katılma teklifi genelde, Uygulamada kaydedilen belirli bazı olaylara (örneğin yüksek risk görüntülenmesi) bağlı olarak sunulur. Ankete katılarak, RKI'nin Uygulamanın etki gücünü değerlendirmesine, Uygulamayı iyileştirmesine ve örneğin Uygulama üzerinden gönderilen uyarıların enfeksiyonu önlemeye katkı verip vermediklerini ve nasıl verdiklerini anlamasına yardımcı olursunuz.

Ankete katılım isteğe bağlıdır. Bir ankete katılmaya ve kullanım verilerinin RKI'ye aktarılmasına, siz kendiniz karar verirsiniz. Bu anketler, yönlendirileceğiniz Uygulama dışındaki bir web sitesinde gerçekleştirilir. Ankete katılım, Uygulamanızın orijinalliğinin doğrulanmasını gerektirir (bu konuyla ilgili daha fazla bilgi için bkz. Madde 5 h. ve 11.).

h. Uygulamanızın orijinalliğinin doğrulanması

Uygulamadaki bazı işlevler, Uygulamanızın orijinalliğinin önceden kontrol edilmesini ve RKI için onaylanmasını gerektirir. Orijinal ürün kontrolü, özellikle Uygulamanın manipüle edilmiş veya tahrif edilmiş ("sahte") bir sürümünü kullanıp kullanmadığınızı belirlemek içindir. Orijinal ürün kontrolü için işletim sisteminizin bir işlevinden yararlanılır. Bu bağlamda akıllı telefonunuz tarafından benzersiz bir kimlik kodu oluşturulur ve bunu işletim sisteminizin üreticisine gönderir (bir Android akıllı telefon kullanıyorsanız, bu veriler Google'a, iPhone kullanıyorsanız Apple'a aktarılır). Bu kimlik kodu, akıllı telefonunuzun sürümü ve Uygulama hakkında veriler içerir. İşletim sisteminizin sağlayıcısı, muhtemelen kimlik kodunuz üzerinden kim olduğunuzu ortaya çıkarabilir ve akıllı telefonunuzun orijinallik kontrolünün yapıldığını anlayabilir. Uygulamadan karşılaşma verileri gibi başka bilgiler İşletim sisteminizin sağlayıcısına gönderilmez. İşletim sisteminin sağlayıcısı, Uygulamanızın orijinal olduğunu RKI'ye doğrulamak için bu kimlik kodunu kullanır. Orijinalliğinin doğrulanmasını sağlayan bu işlevin kullanılması isteğe bağlıdır. Ancak Uygulamanızın orijinalliğinin doğrulanmasını kabul etmezseniz, Uygulamanın başka bazı işlevleri sizin için sunulmayabilir.

6. Verileriniz niçin işleniyor?

a. Risk değerlendirmesi

Uygulamanın ana işlevlerinden biri, risk değerlendirmesidir. Bunun görevleri, Korona testi pozitif çıkan kişilerle olası maruz kalmaları (riskli karşılaşmalar) konusunda sizi sınır ötesi ortamda da uyarmak, kişisel enfeksiyon riskinizi hesaplamak ve size bu bağlamda davranış ve sağlık bilgileri temin etmektir.

Bu amaç doğrultusunda Uygulama, arka planda çalışarak sunucu sisteminden, Korona testi pozitif çıkan ve sınır ötesi uyarı sistemine katılan ülkelerin resmi Korona uygulamaları aracılığıyla bir uyarı tetikleyen kullanıcılardan rastgele kimlik numaraları ve varsa semptomların başlangıcına ilişkin bilgiyi içeren listeleri günde birçok kez 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 pozitif listeden aldığı bu rastgele kimlik numaralarını, COVID-19 bildirim sistemine aktarır ve bu sistem bu kodları, karşılaşmalarınızda 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 maruz kalma verileri ve pozitif listedeki bilgiler (taşıma riski değeri, semptomların başlangıcına ilişkin bilgiler) enfeksiyon riskinizi belirlemek için Uygulama tarafından değerlendirmeye alınır. Bu veriler için olan değerlendirme kuralları, RKI'nin güncel bilimsel bulgularına (örn. temas süresinin enfeksiyon riski üzerindeki etkisi) dayanmaktadır. Yeni bulgular olması durumunda RKI, Uygulamanın değerlendirme ayarları üzerinden bu değerlendirme kurallarını güncelleyebilmektedir. Bu durumda, yeni değerlendirme ayarları pozitif listeyle 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.

Sizin için bir enfeksiyon riski hesaplanırsa, bu değer Uygulamada görüntülenecektir. Görüntülenen bu risk değeri yüksek ise, bunun anlamı, sizin Korona testi pozitif çıkan ve bir uyarı tetikleyen diğer kullanıcılarla bir veya daha çok kez karşılaşmış olmanızdır. Son 14 gün için hesaplanan risk, iletişim günlüğünün takvim görünümünde görüntülenir. Lütfen riskin kaynağıyla ilgili yanlış çıkarımlar yapmaktan kaçının: Belli bir gün için hesaplanan ve görüntülenen bir risk, tanımadığınız kullanıcılarla farkına varmadığınız bir karşılaşmaya kadar geri gidebilir ve mutlaka iletişim günlüğüne girdiğiniz kişiler veya yerlerle ilgili olması gerekmez.

b. Test sonucu çağırın

Bir korona testi yaptırdıysanız, test sonucunuzu Uygulama üzerinden görüntüleyebilirsiniz. Test sonucunuz hazır olur olmaz, Uygulama sizi bu konuda bilgilendirecektir. Ancak bu bilgilendirme, test laboratuvarının sunucu sistemine bağlı olmasını ve ayrıca test süreci kapsamında sizin test sonuçlarınızın aktarılmasına onay vermenizi gerektirir. Uygulamanın sunucu sistemine bağlı olmayan laboratuvarlardan gönderilen test sonuçları görüntülenemez. Bir QR kod almadıysanız, bu işlevi yine aynı şekilde kullanamazsınız.

<u>QR kodu tarayın</u>

Test sonucunu Uygulama aracılığıyla çağırmak için, bu QR kodu akıllı telefonunuzun kamerasıyla taramanız gerekir. Bu QR kod, bir kod numarası içerir, bu kod numarası tarama işlemiyle okunur ve testinize ataması yapılır. 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. Bu karma kod numarasının test sonucunuza benzersiz olarak atanması, hâlâ mümkündür. Akıllı telefonunuz internete bağlanır bağlanmaz, Uygulama bu karma kod numarasını sunucu sistemine iletir. Bunun üzerine sunucu sistemi bir dijital erişim kodu, yani bir belirteç (token) sunar ve bu belirteç Uygulamaya kaydedilir. Belirteç, sunucu sistemindeki karma kod numarasına bağlıdır. Uygulama daha sonra akıllı telefonunuzdaki karma kod numarasını siler ve sadece belirteci tutar. Böylece QR kod artık kullanılmış (geçersiz) olur, yani artık kimse tarafından kullanılamaz. Bu sayede QR kodunuzun test sonucunu sorgulamak için başka bir kullanıcı tarafından kullanılmasının önüne geçilmiş olur.

<u>Test sonucunun saklanması</u>

Test sonucunuz test laboratuvarında hazır olduğunda, bu sonucu hemen 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, aynı matematik yöntemini kullanarak, size verilen QR kodda yer alan kod numarası bazında karma kod numarasını oluşturur.

Test sonucunun çağrılması

Uygulama, düzenli olarak Uygulamada kaydedilmiş olan belirteci kullanarak sunucu sisteminden kayıtlı testinizin durumunu sorgular. Sunucu sistemi, Uygulamaya testinizin güncel durumunu (sonuç hazır / sonuç hazır değil) paylaşır. Test sonucunuz hazır olduğunda, ilgili tanı (Korona pozitif veya Korona negatif) Uygulamaya iletilir. Uygulamadaki test durumu bildirimlerini etkinleştirdiyseniz ("Ayarlar" > "Bildirimler" altında), söz konusu bildirimi alırsınız. Ancak Uygulamayı açtıktan sonra, test sonucu size gösterilir.

Korona testiniz pozitif çıkmışsa, Uygulama, tekrar belirteci kullanarak sunucu sisteminden bir TAN (işlem numarası) ister. Bu TAN kodu, diğer kullanıcılara yanlış uyarı verilmesini önlemek için gereklidir. 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. Diğerlerini uyarın

Korona testiniz pozitif çıkmışsa ve siz rastgele kimlik numaralarınızı Uygulama aracılığıyla paylaşırsanız, bu Uygulamanın veya diğer resmi Korona uygulamalarının kullanıcılarıyla bir karşılaşma söz konusu olduğunda, bu kişilerin uyarılması sağlanır. 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.)

Test sonuçlarınız sunucu sistemine aktarılmadan (daha doğrusu, rastgele kimlik numaralarınızın aktarımından) önce, Uygulama, verilere bir taşıma riski değeri ve gerçekleştirilen test tipi hakkında bilgi ekler. Uygulamanın uyarı işlevi, sadece laboratuvarda onaylanan test sonuçlarında kullanılabildiğinden, test tipi tüm kullanıcılar için aynıdır. Taşıma riski değeri, 14 günlük dönemin her bir günündeki 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. Bu ek taşıma riski değerleri, diğer kullanıcılar için enfeksiyon olasılığının daha kesin bir şekilde belirlenmesini mümkün kılar.

Uygulamada sorgulanan semptomların başlangıcına ilişkin bilginin verilmesi, isteğe bağlıdır. Ancak bu bilgi, taşıma riski değerinin daha da 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 de o kadar küçük olur.

Uygulama üzerinden test sonucunuzu almadıysanız:

Pozitif test sonucunuzu Uygulama üzerinden çağırmamış 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 gerçekten 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 benzersiz TeleTAN'ınızı oluşturacak ve bu konuda bilgi vermek için sizi arayacaktır. Bir TeleTAN yalnızca bir saat süreyle geçerli kalır ve dolayısıyla size iletildikten hemen sonra, ancak en geç bir saat içinde yardım hattındaki sistemden silinir. Uygulamaya geçerli bir TeleTAN girildikten sonra, bu kod sunucu sistemine iletilir. TeleTAN'ın kullanımı sayesinde gerçekten pozitif bir test sonucu olup olmadığını kontrol etmek ve böylece yanlış mesajları önlemek mümkün olur. Bunun ardından geçerli bir QR kodunu taranmasında olduğu gibi (Madde 6 b "Test sonuçlarının çağrılması"na bakın), Uygulama, sunucu sisteminden bir belirteç alır.

Bazı nadir durumlarda, verdiğiniz bir uyarının, kişisel çevrenizde bu Uygulamayı kullanan ve uyarılmış kişilerin, bu uyarıyı sizin verdiğiniz sonucuna varabileceğini lütfen göz önünde bulundurun. Böyle bir durum örneğin, kendi kişisel çevrenizdeki bir kişinin, riskli karşılaşmanın bildirildiği gün, sizin dışınızda başka bir temas kurmaması halinde söz konusu olabilir.

d. Uygulamanın bilgilenme amaçlı kullanımı

Uygulama otomatik olarak sunucu sistemi üzerinden günlük istatistikleri alır ve bunlar Uygulamada görüntülenir. Bu sırada erişim verileri oluşur. 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.

e. Temas günlüğü

Temas günlüğü, Uygulamanın ek bir işlevidir. Temas günlüğündeki veriler, bir hatırlatma görevi görür ve yalnızca sizin tarafınızdan erişilebilir. Daha sonraki bir tarihte Korona testiniz pozitif çıkarsa ve sağlık kurumu sizden temas takibinde yardım etmenizi rica ederse, sağlık kurumuna temas takibi için gerekli bilgileri hızlı bir şekilde aktarabilirsiniz. Belli bir gün yüksek risk altında olduğunuzun saptanması halinde, böyle bir günde sizin için hesaplanan riskin görüntülenmesi, temas ettiğiniz kişileri veya size eşlik etmiş olan kişileri uyarmanıza yardımcı olabilir. Bu sayede temaslı kişileriniz, gerektiğinde kendi temas davranışlarını bu duruma ayarlayabilir ve böylece kendi çevrelerinde henüz saptanmamış olası enfeksiyonların önüne geçebilir.

f. Veri bağışı

Veri bağışı kapsamında RKI'ye aktarılan kullanım verileri ve diğer isteğe bağlı veriler, Uygulamanın etki gücünü ölçmek ve aşağıda sıralanan iyileştirmeleri sağlamak üzere değerlendirmeler yapmak üzere kullanılır:

- Risk değerlendirmesinin iyileştirilmesi - Enfeksiyon riskinin teknik hesaplamasının doğruluğu ve güvenilirliğinin iyileştirilmesi hedeflenir. Bunun için riskli karşılaşmalarla ilgili veriler ve size görüntülenen uyarılar değerlendirilir. Buna dayanarak hesaplama yöntemi iyileştirilebilmektedir.
- Uygulamadaki kullanıcı kılavuzluğunun iyileştirilmesi - Uygulama kullanımının daha kolay olması hedeflenir. Bu bağlamda kullanıcıların Uygulamadaki bireysel adımlarına ilişkin veriler değerlendirilir. Bu sayede etiketlemeler ve uyarı notları daha anlaşılır hale getirilebilir ve kumanda elemanları daha kolay bulunabilecek şekilde

konumlandırılabilir. Ayrıca Uygulama gösterimlerinin, farklı akıllı telefon modellerine uyarlanması mümkün olur.

- Uygulamaya ilişkin bilgilendirme ve yardımın sağlanması - Testlerin yapıldığı belirli tesisler ve laboratuvarlarla bağlantılı olarak veya belirli coğrafi bölgelerde Uygulamanın kullanımıyla ilgili olası sorunların varlığını saptamak hedeflenir. Böylece veri bağışı nedeniyle örneğin, test sonuçlarının belirli coğrafi bölgelerde geç elde edileceğinin farkına varmak mümkün olabilir. Bu sayede sorumlu sağlık kurumu yetkilileri de olası teknik arızalar hakkında bilgilendirilebilmektedir.
- Pandemi seyrine ilişkin istatistiklerin iyileştirilmesi - Bu veriler, pandeminin seyrine ilişkin belirli olayların zaman ve mekân açılarından dağılımı ile ilgili bilgi verebilir ve belli bazı olayların gelişmesine daha hızlı tepki verilmesini sağlayabilir.

Kullanım verileri ve diğer isteğe bağlı veriler, adınız veya kimliğinizle herhangi bir bağlantı olmaksızın saklanır ve değerlendirilir. RKI, kim olduğunuzu veya kiminle karşılaştığınızı öğrenmez.

g. Hata raporları

RKI, hatasız bir Uygulama sunmayı hedeflemektedir. Ancak, çok sayıda farklı sistem nedeniyle bu hedefe her zaman ulaşılmayabilmektedir. Hata analizi ile ilgili olarak Uygulama teknik desteğine yardımcı olmak için, Uygulamanızda hata raporu oluşturup RKI'ye aktarabilirsiniz. RKI, Uygulamanızda ortaya çıkan hataların nedenlerini belirlemek ve bunları gidermek için hata raporunu değerlendirmeye alacaktır.

Bu hata raporları, adınız ve kimliğiniz ile herhangi bir bağlam olmaksızın geçici olarak saklanır ve hata analizi kapsamında değerlendirilir. RKI, kim olduğunuzu veya kiminle karşılaştığınızı öğrenmez. Ancak hata raporunu teknik desteğe iletirken, hata raporu kimlik numarasını ifşa ederseniz (örn. e-posta yoluyla), bu işlemin kimliğiniz hakkında ipuçları ortaya çıkarabileceğini göz önünde bulundurun.

h. Anketler

Anketler, Uygulama dışında yönlendirileceğiniz bir web sitesinde gerçekleştirilir. Uygulama, anketlerle bağlantılı olarak RKI'ye veri aktarımı sağlamaz. RKI tarafından yürütülen anketlerin amaçları, anket web sitesinde anketteki bilgilerde yer almaktadır.

i. Uygulamanızın orijinalliğinin doğrulanması

Uygulamanızın orijinalliğinin doğrulanması için akıllı telefonunuzun işletim sisteminin bir işlevi kullanılır. Bu sayede sadece uygulaması düzgün çalışan Uygulama kullanıcılarının veri bağışına veya anketlere katılması mümkün kılınır. Böylece istatistiklerin ve anket sonuçlarının tahrif edilmesinin önüne geçilir.

Lütfen işletim sisteminizin sağlayıcısının muhtemelen akıllı telefonunuzun orijinallik kontrolünün yapıldığını anlayabileceğini ve bu nedenle kimliğinizi ortaya çıkarabileceğini unutmayın. Ancak, işletim sisteminizin sağlayıcısı Corona-Warn-App kullanımınız hakkında daha fazla bilgi almaz.

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 uyarı sunucuları (bundan böyle: **veri değişim sunucusu**) kurmuştur.

- Avrupa Birliği üye devletlerinden katılımcı ülkelerin veri değişim sunucusu, üye devletler ile AB arasındaki elektronik sağlık hizmetleri iletişim ağının dijital altyapısını kullanır.
- RKI bu değişim sunucusu dışında ayrıca, İsviçre Corona-App ve Corona-Warn-App kullanıcıları arasında da uyarıların iletilebilmesi için, İsviçre (İsviçre Konfederasyonu Federal Sağlık Dairesi) ile birlikte başka bir değişim sunucusu işletmektedir.

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

İlgili sunucu sistemi, aldığı pozitif listeleri kendi pozitif listesiyle birleştirir, bu sayede risk değerlendirmesinde, 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.

Veri değişim sunucularına, 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.

- AB içinde işletilen veri değişim sunucusuna ilişkin iş birliğinin teknik ve organizasyonel ayrıntıları AB Komisyonunun bir kararında belirlenmiştir (15 Temmuz 2020 tarihli Uygulama Kararı (AB) 2020/1023, bu karara https://eur-lex.europa.eu/eli/dec_impl/2020/1023/oj) adresinden erişebilirsiniz. RKI ve katılımcı ülkelerin yetkili sağlık kurumları, sınır ötesi risk değerlendirmesi ve uyarısı sağlamak üzere veri değişim sunucularında bulunan pozitif listelerde yer alan verilerin (rastgele kimlik numaraları ve semptomların başlangıcına ilişkin olası bilgiler) işlenmesinden müştereken sorumludur.
- İsviçre ile ortaklaşa işletilen veri değişim sunucusunun çalışması ve veri alışverişi, RKI ve İsviçre arasında özel bir anlaşmada düzenlenmekte olup, ayrıntıları https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Warn_App.html adresinden erişilebilir. Veri değişim sunucusunun teknik işletimi, İsviçre Federal Sağlık Dairesi tarafından gerçekleştirilmektedir. Pozitif listelerin saklanması, sağlanması ve daha sonra silinmesinden, RKI ve İsviçre Federal Halk Sağlığı Dairesi müştereken sorumludur.

Sisteme katılımcı ülkeler listesinin değişebileceğini, lütfen göz önünde bulundurun. İlgili sorumlu sağlık kurumları hakkında bilgilerin bulunduğu güncel listenin yer aldığı sıkça sorulan sorulara https://www.coronawarn.app/de/faq/#interoperability_countries adresinden 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 hesaplamak 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:

- "Test sonucu çağırın" 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 sonucunuzun durumundaki değişikliklerden haberdar olmak için, bildirimler işlevi etkinleştirilmiş olmalıdır.

Bunlara ek olarak Uygulama aşağıdaki yetkilere gerek duyar:

- "Test sonucu çağırın" 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, 14 güne kadar süren inkübasyon dönemi (hastalığın bulaşmasından hastalığın başlangıcına kadar geçen süre) 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

Pozitif listeler 14 gün geçtikten sonra Uygulama belleğinden silinir. Sizin için Uygulamada hesaplanan enfeksiyon riski (örn. "düşük risk"), her güncellemeden sonra, ancak en geç 14 gün sonra Uygulama belleğinden silinir. Çağırdığınız Korona testi pozitif ise ve siz bir uyarı tetikledikten hemen sonra belirteç, Uygulama belleğinden silinir. Temas günlüğündeki veriler akıllı telefonunuzda 16 gün boyunca saklanır ve ardından otomatik olarak silinir. Ancak bu verileri istediğiniz zaman, daha erken de silebilirsiniz.

b. Sunucu sistemlerindeki veriler

Pozitif listeler, 14 gün sonra tüm sunucu sistemlerinden (değişim sunucuları dahil) silinir. Veri bağışı kapsamında ve Uygulamanızın orijinalliğinin doğrulanması için aktarılan veriler haricinde diğer tüm veriler en geç 21 gün sonra silinir.

c. Veri bağışı

Veri bağışı kapsamında RKI'ye aktarılan kullanım verileri ve diğer isteğe bağlı veriler 180 gün sonra silinir.

d. Hata raporları

Akıllı telefonunuzda kaydedilmiş bir hata raporunu istediğiniz zaman silebilirsiniz. Teknik desteğe göndermiş olduğunuz hata raporları ise en geç 14 gün sonra silinecektir.

e. Uygulamanızın orijinalliğinin doğrulanması

Uygulamanızın orijinalliğini doğrulamak için akıllı telefonunuzun oluşturduğu kimlik kodları, RKI'ye gönderildikten 30 gün sonra sunucu sistemlerinden silinir.

10. Verileriniz kime aktarılır?

Uygulama aracılığıyla diğer kullanıcıları uyardığınızda, test sonucunuz son 14 güne ait rastgele kimlik numaralarınız halinde ve semptomların başlangıcına ilişkin isteğe bağlı bilgiler, veri değişim sunucularına 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, bu verileri pozitif listelerin bir ögesi olarak kendi kullanıcılarına dağıtır.

Katılımcı AB ülkelerinin yetkili ulusal sağlık kurumları, ortaklaşa işletilen uyarı sisteminin işletimi ve bakımı için AB Komisyonuna işletici kuruluş olarak yetki vermiştir. Corona-Warn-App ile İsviçre Corona-App arasında gerçekleşen sınır ötesi uyarılar ile ilgili olarak veri değişim

sunucusu, RKI ile koordineli olarak İsviçre Federal Sağlık Dairesi tarafından işletilir ve bakımı yapılır.

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 RKI tarafından veri aktarımı gerçekleşmez.

11. Verileriniz AB dışındaki ülkelere aktarılacak mı?

Bir uyarıyı tetiklediğinizde, rastgele kimlik numaralarınız, İsviçre Federal Sağlık Dairesi ile birlikte RKI tarafından işletilen İsviçre'deki veri değişim sunucusuna da gönderilir. AB, İsviçre veri koruma seviyesinin yeterliliğinin belirlendiği bir yeterlilik kararı çıkarmıştır (GVKT madde 45). Bundan başka güncel pozitif listeler, kullanıcının konumundan bağımsız olarak (örneğin tatilde veya iş gezisinde) çağrılır. Ayrıca, Uygulamanızın orijinalliğinin doğrulanması kapsamında verilerin AB dışındaki bir ülkeye aktarılması söz konusu olabilir. Akıllı telefonunuz tarafından oluşturulan ve akıllı telefonunuzun ve Uygulamanın sürümüyle ilgili bilgileri içeren kimlik kodu, akıllı telefonunuzun işletim sisteminin sağlayıcısına (Apple veya Google) aktarılır. Bu süreçte verilerin üçüncü ülkelere, özellikle ABD'ye aktarılması da söz konusu olabilir. Orada muhtemelen Avrupa hukuku standartlarına uygun kişisel verilerin koruma seviyesi bulunmayabilir ve Avrupa'daki veri koruma haklarınız uygulanmayabilir. Bu bağlamda özellikle üçüncü ülke güvenlik makamlarının işletim sistemi sağlayıcısına aktarılan bu verilere erişme ve örneğin verileri diğer bilgilerle ilişkilendirerek bunları değerlendirmeye alma olasılığı bulunmaktadır. Ancak bu, yalnızca aktarılan kimlik kodlarını etkiler. Karşılaşma verileri gibi Uygulamadaki diğer veriler bu prosedüre dahil edilmez.

Ancak Uygulama tarafından aktarılan veriler, sadece Almanya'daki sunucularda veya bir diğer AB (veya Avrupa Ekonomik Alanı) ülkesindeki sunucularda işlenir, dolayısıyla Genel Veri Koruma Tüzüğünün (GVKT) katı gerekliliklerine tabi kalır.

12. Verdiğiniz rıza beyanını nasıl geri alabilirsiniz?

Geleceğe dönük geçerli olmak üzere, Uygulamada RKI'ye verdiğiniz bir onayı istediğiniz zaman geri alma hakkına sahipsiniz. Bununla birlikte, verileriniz işlenmesi halen gerçekleştirilmiş ise artık bu işlemler geri alınamaz. RKI'nin, özellikle akıllı telefonlardan diğer kullanıcılara halen aktarılmış olan rastgele kimlik numaralarını silme olanağı yoktur.

a. Maruz kalma günlüğüne ilişkin rıza beyanı

Maruz kalma günlüğüne vermiş olduğunuz rıza beyanını, istediğiniz zaman Uygulamadaki kaydırıcıyı kullanarak, işlevi devre dışı bırakabilir veya Uygulamayı silerek iptal edebilirsiniz. Risk değerlendirmesini tekrar kullanmak isterseniz, kaydırıcıyı yeniden etkinleştirebilir veya Uygulamayı yeniden yükleyebilirsiniz.

b. “Test sonucunu çağırın” işlevine dair rıza beyanı

Uygulamanın test sonucunu çağırması için verdiğiniz rıza beyanını, testi Uygulamada görüntüleyip, sonra kaldırarak iptal edebilirsiniz. Bunun ardından test sonucunu çağırmak için kullanılan belirteç, Uygulama belleğinden silinir, böylece belirteç artık sunucu sisteminde atanamaz. Aynı testi Uygulamanıza yeniden atamanız veya aynı QR kodu yeniden taramanız mümkün değildir. Yeniden bir test yaptırırsanız ve test sonucunu görmek isterseniz, yeniden buna dair rıza beyanında bulunmanız istenecektir. Ancak test sonucu Uygulamada halen mevcutsa, ilgili rıza beyanı artık geri alınamaz.

c. “Diğerlerini uyarın” işlevine dair rıza beyanı

Diğer insanları uyarmak için test sonucunuzun (daha doğrusu, son birkaç güne dair rastgele kimlik numaralarınız) aktarılmasına ilişkin vermiş olduğunuz rıza beyanını, testi görüntüleyerek ve ardından “Diğerlerini Uyarın” seçeneğinin devre dışı bırakarak iptal edebilirsiniz. Bu olanak, diğer kullanıcıları uyarmak için henüz rastgele kimlik numaralarınızı göndermediğiniz sürece söz konusudur.

Rastgele kimlik numaralarınızı gönderdikten sonra, verdiğiniz rıza beyanını geri almanın tek yolu Uygulamayı silmektir. Sunucu sistemine halen iletilmiş olan rastgele kimlik numaralarınız, Uygulama belleğinden silinecek ve böylece artık size veya akıllı telefonunuza atanamayacaktır. Daha sonra tekrar bir uyarı tetiklemek isterseniz, Uygulamayı yeniden yüklemeniz ve tekrar rıza beyanında bulunmanız gerekecektir. Halen Uygulamanıza atanmış olan ve diğer insanları uyarmak için gönderilen bir test sonucu, diğerlerini uyarmak için yeniden kullanılamaz.

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

d. “Veri bağışı” rıza beyanı

Uygulamanın ayarlarından “Verileri bağışla” seçeneğini devre dışı bırakarak, istediğiniz zaman vermiş olduğunuz rızayı geri alabilirsiniz. Bunun ardından Uygulama, artık kullanım verilerinizi ve diğer isteğe bağlı verileri günlük olarak RKI’ye aktarmayacaktır. Daha sonra veri bağışına yeniden izin vermek isterseniz, ilgili işlevi ayarlardan yeniden etkinleştirebilirsiniz.

e. “Hata raporları” rıza beyanı

Daha önceden RKI’ye gönderdiğiniz hata raporlarının analizi için olan rıza beyanınızı geri çekebilirsiniz, bunun için teknik desteğe hata raporu kimlik numaranızı belirterek, hata raporunun artık analiz edilmesini istemediğinizi bildirmeniz yeterlidir. Bunun üzerine hata raporunuz silinir. RKI’nin bu prosedürde kimliğinizi öğrenebileceğini göz önünde bulundurun. Hata raporu kimlik numaranızı teknik destek aktarmazsanız, gönderilen hata raporu 14 gün sonra otomatik olarak silinecektir.

f. “Anket” rıza beyanı

Bir RKI anketine katılmak için gereken rızanızı, Uygulamada değil, anketin gerçekleştirildiği web sitesi üzerinden verirsiniz. Orada, verdiğiniz rızayı nasıl geri alabileceğinize ilişkin bir açıklama da bulunmaktadır.

g. “Uygulamanızın orijinalliğinin doğrulanması” rıza beyanı

Uygulamanızın orijinalliğinin doğrulanması için verdiğiniz rızayı geri alırsanız, bunun ilgili veri işleme üzerinde doğrudan herhangi bir etkisi yoktur. Siz bu rızanızı verdikten hemen sonra, akıllı telefonunuz tarafından oluşturulan kimlik kodu, işletim sisteminizin sağlayıcısına aktarılır ve Uygulamanızın orijinalliğinin doğrulanması ve onaylanması orada gerçekleşir.

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,
- resmi RKI’nin veri koruma görevlisi ile iletişim geçme ve isteklerinizi dile getirme hakkı (GVKT madde 38, fıkra 4 uyarınca) ve
- 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, diğer insanları uyarmak için son birkaç güne ait rastgele kimliklerinizi gönderdiğiniz sürece (Madde 7’ye bakın), veri değişim sunucularına katılan ülkelerdeki veri işlemeden sorumlu sağlık kurumları tarafından da size tanınmaktadır.

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.