Veri Sorumlusu Olarak Bağlayıcı Şirket Kuralları

|  |
| --- |
| Bağlayıcı Şirket Kuralları Veri Sorumlusu dokümanı, Avrupa Lider Kuruluşu olarak hareket eden Webhelp SAS çatısı altında bulunan Concentrix iştiraki için geçerlidir.  Bağlayıcı Şirket Kurallarının uygulandığı İştirakler, BCR Ek 01’de listelenmiştir. |

İçindekiler

[1. Giriş 3](#_Toc177054187)

[2. Kapsam 4](#_Toc177054188)

[2.1 Maddi kapsam 4](#_Toc177054189)

[2.2 Coğrafi kapsam 5](#_Toc177054190)

[3. Bağlayıcı Mahiyet 5](#_Toc177054191)

[3.1 Concentrix çalışanları üzerinde 5](#_Toc177054192)

[3.2 Concentrix Grubunun BCR Üyeleri üzerinde 6](#_Toc177054193)

[3.3 Concentrix Veri İşleyenlerine karşı 6](#_Toc177054194)

[4. Kişisel verilerin işlenmesine ilişkin ilkeler 7](#_Toc177054195)

[4.1 Veri İşleme için yasal bir dayanak tanımlama (Şeffaflık, adalet ve yasaya uygunluk) 8](#_Toc177054196)

[4.2 Bir amacın tanımlanması (Amaç sınırlaması) 8](#_Toc177054197)

[4.3 Kişisel Veri toplamanın en aza indirilmesi (Verilerin asgariye indirilmesi) 9](#_Toc177054198)

[4.4 Kayıt tutma 9](#_Toc177054199)

[4.5 Kişisel Verilerin Doğruluğu (Veri Doğruluğu) 10](#_Toc177054200)

[4.6 Veri saklama süresinin tanımlanması (Sınırlı saklama süresi) 10](#_Toc177054201)

[4.7 Güvenlik önlemlerinin uygulanması (bütünlük ve gizlilik) 10](#_Toc177054202)

[4.8 Veri Koruma Etki Değerlendirmesi 11](#_Toc177054203)

[4.9 Concentrix Grubu Dışındaki Alt Veri İşleme ve Veri Aktarımları 12](#_Toc177054204)

[4.10 Kişisel Veri İhlali bildirim önlemlerinin uygulanması 12](#_Toc177054205)

[5. Hassas verilerin işlenmesi 13](#_Toc177054206)

[6. Kişisel Verilerin üçüncü ülkelere aktarılması ve BCR Üyesi Olmayanlara ileriye dönük Aktarım kısıtlaması 14](#_Toc177054207)

[6.1 Kişisel Veri Aktarımları ve ileriye dönük Aktarımlar 14](#_Toc177054208)

[6.2 Devletin erişim talebi durumunda Veri Alıcısının yükümlülüğü 15](#_Toc177054209)

[7. İlgili Kişinin Hakları 16](#_Toc177054210)

[7.1 Üçüncü Taraf Lehtar Hakları 16](#_Toc177054211)

[7.2 AEA içindeki bir BCR Üyesinin BCR-C’ye uymaması durumunda şikayette bulunma ve yargısal çözüm, düzeltme ve tazminat alma hakkı 17](#_Toc177054212)

[7.3 AEA dışındaki bir BCR Üyesinin BCR-C’ye uymaması durumunda şikayette bulunma ve yargısal çözüm, düzeltme ve tazminat alma hakkı 18](#_Toc177054213)

[7.4 İlgili Kişilerin Hakları 19](#_Toc177054214)

[7.5 İlgili Kişilerin Haklarının Kullanılması 19](#_Toc177054215)

[8. İlgili Kişilerin şikayet yönetimi prosedürü 21](#_Toc177054216)

[9. Veri koruma yönetimi 22](#_Toc177054217)

[10. Eğitim ve farkındalık 22](#_Toc177054218)

[11. Kasten gizlilik/varsayılan gizlilik 23](#_Toc177054219)

[12. Şeffaflık ve işbirliği 24](#_Toc177054220)

[12.1 BCR-C İletişimi 24](#_Toc177054221)

[12.2 İlgili Kişilere Sağlanan Bilgiler 25](#_Toc177054222)

[12.3 BCR-C'ye uyumu etkileyen yerel mevzuat ve uygulamalarla tutarsızlıklar 26](#_Toc177054223)

[12.4 İşbirliği yapma görevi 28](#_Toc177054224)

[13. BCR’yi kapsayan denetim programı 28](#_Toc177054225)

[14. BCR-C’de değişiklik 30](#_Toc177054226)

[15. BCR-C'ye uyulmaması 30](#_Toc177054227)

[16. Fesih 31](#_Toc177054228)

[17. Ekler 32](#_Toc177054229)

[BELGE KONTROLÜ 33](#_Toc177054230)

1. Giriş

|  |
| --- |
| **Hatırlatıcı:** **Eylül 2023 tarihinde gerçekleşen Webhelp & Concentrix işleminin ardından, grubun ticari adı artık Concentrix olarak belirlenmiştir. Bununla birlikte, mevcut Bağlayıcı Şirket Kuralları (BCR) kapsamının değiştirilmediğini lütfen unutmayınız. Bağlayıcı Şirket Kuralları yalnızca Avrupa Lider Kuruluşu olarak hareket eden Webhelp SAS çatısı altındaki İştirakler için geçerlidir. Bağlayıcı Şirket Kurallarına (Veri Sorumlusu ve/veya Veri İşleyen) tabi olan İştirakler, Ek 01’de listelenmiş olup BCR Üyesi olarak anılacaktır.** |

Concentrix Grubu olarak, Kişisel Verilerin korunmasının yalnızca bir güvenlik veya belirli bir yasal çerçeveye uyum meselesi olmadığına, daha ziyade bireysel ve kurumsal bir taahhüt meselesi olduğuna inanıyoruz. Concentrix standartlarının Veri İşleyenler için Bağlayıcı Şirket Kuralları (bundan böyle “BCR-P”) ve işbu Veri Sorumluları için Bağlayıcı Şirket Kuralları (bundan böyle “BCR-C”) vasıtasıyla açıklanması ve paylaşılması, İlgili Kişilerin Kişisel Verilerinin nasıl İşlendiğine ilişkin meşru beklentileri açısından son derece önemlidir.

BCR Üyeleri faaliyetleri sırasında hem kurum içi verileri hem de Müşterinin Kişisel Verilerini işlerler. Bu bağlamda, BCR Üyeleri kendi adına işlediği Kişisel Verileri işbu BCR-C dokümanında yer alan uygun teknik, fiziki ve idari önlem ve kontrollerin uygulanması suretiyle korurlar. Söz konusu kontroller, tüm kuruluşun Veri İşlemenin niteliğini ve/veya yerini dikkate almadan Kişisel Verileri tutarlı bir şekilde İşlemesini sağlayacaktır.

Bu yaklaşım, Concentrix’in Müşterileri adına ele aldığı faaliyetlerin çeşitliliği nedeniyle özellikle önemlidir.

Yukarıdaki hususların bir sonucu olarak ve 27 Nisan 2016 tarihinde kabul edilen 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü (bundan böyle “**EU Tüzüğü”** veya **"GDPR"**) ile getirilen gerekliliklerin yanı sıra AB Tüzüğü ile çelişmediği takdirde veri koruma alanında yürürlükte olan standart, yönetmelik ve yasaları dikkate alarak, BCR Üyeleri Kişisel Verileri aşağıdaki ilkeler doğrultusunda İşleyecektir:

* **Yasaya Uygunluk** – Kişisel Veriler, İlgili Kişi tarafından Veri İşlemeye onay verildiği takdirde veya söz konusu Veri İşleme Yürürlükteki Veri Koruma Mevzuatı uyarınca meşru veya gerekli olduğunda toplanacak ve İşlenecektir.
* **Adalet** – Kişisel Verilerin İşlenmesinde söz konusu Kişisel Verilerin İşlendiği özel koşullar ve bağlam dikkate alınacaktır.
* **Şeffaflık** – Kişisel Verilerin İşlenmesine ilişkin bilgi ve iletişim kolay erişilebilir, kolay anlaşılır, net, açık ve sade bir dille olmalıdır.
* **Amaç sınırlaması** – Kişisel Veriler belirli, açık ve meşru amaçlar için toplanacak olup bu amaçlarla bağdaşmayan bir şekilde daha fazla İşlenmeyecektir.
* **Verilerin asgariye indirilmesi** – Toplanan Kişisel Veriler, İşlendikleri amaçlar doğrultusunda yeterli, alakalı ve gerekli olanlarla sınırlı olacaktır.
* **Doğruluk** – Kişisel Veriler doğru olacak ve gerektiğinde güncel tutulacaktır. Veri işleme amaçları göz önüne alındığında, doğru olmayan Kişisel Verilerin fazla gecikmeden silinmesini veya düzeltilmesini sağlayacak her makul adım atılmalıdır.
* **Saklama sınırlaması** – Kişisel Veriler, söz konusu verilerin İşlenme amaçları veya diğer yasal saklama süreleri için gerekenden daha uzun süre İlgili Kişilerin kimlik tespitine olanak tanıyan bir biçimde tutulmayacaktır.
* **Bütünlük ve gizlilik** – Kişisel Veriler uygun teknik, fiziki ve idari önlemlerin uygulanması suretiyle yetkisiz veya kanuna aykırı Veri İşleme süreçlerine ve Kişisel Verilerin kazayla kaybedilmesi, imha edilmesi veya zarar görmesi gibi durumlara karşı koruma da dahil olmak üzere Kişisel Verilerin güvenliğini sağlayacak şekilde işlenecektir.

Concentrix, işbu BCR-C dokümanı vasıtasıyla tüm BCR Üyeleri için geçerli olan ayrıntı ve ilkeleri paylaşmayı, belirtmeyi ve BCR-C’nin uygulanmasına imkan tanıyan grup çapında belirli standartları sağlamayı amaçlar. Ayrıca Concentrix özel, yerel veya sektörel politikalar da sunabilir. İşbu BCR-C dokümanı ile söz konusu özel, yerel veya sektörel politikalar arasında bir çelişki olması durumunda, bu özel, yerel veya sektörel politikaların çelişkili hükümleri İlgili Kişinin haklarını ve özgürlüğünü daha fazla korumadığı sürece, BCR-C hükümleri esas alınacaktır.

BCR-C, Kişisel Verilerin İşlenmesine ilişkin tüm Concentrix kuruluşu genelinde yeterli ve tutarlı bir yaklaşım sağlamayı amaçladığından, yürürlükteki mevzuatlardan kaynaklanabilecek istisnalar işbu BCR-C dokümanında yansıtılmamıştır. Bununla birlikte, ulusal mevzuatın bir BCR Üyesinin BCR-C’ye uymasını engellediği ve AB Üye Devletlerinin AB Tüzüğüne özel kurallar eklediği durumlarda işbu BCR-C dokümanı, bölüm 12.3’de bir bildirim mekanizması içermektedir. Sonuç olarak, yerel mevzuat, işbu BCR-C için yürürlüğe konabilir bir istisna olarak kabul edilecek ve uygun bildirimin ardından buna göre kaydedilecektir. Bölüm 12.3’te belirtildiği üzere, ulusal mevzuatın Kişisel Veriler için daha yüksek düzeyde bir koruma sağladığı durumlarda bu ulusal mevzuat, BCR-C'ye göre öncelikli olacaktır.

1. Kapsam
   1. Maddi kapsam

İşbu BCR-C, bir BCR Üyesinin Kişisel Verileri Veri Sorumlusu olarak veya Concentrix kuruluşu bünyesinde Veri Sorumlusu olarak hareket eden bir BCR Üyesi adına gerçekleştirilen Veri İşlemede Veri İşleyen olarak İşlediği her durumda geçerlidir.

Concentrix, kendi kapsamına giren çok çeşitli faaliyetler nedeniyle aşağıdakiler gibi muhtelif ve sürekli olarak gelişen Kişisel Veri kategorilerini işlemek zorunda kalabilir:

Kişisel hayata ilişkin veriler (ör. işe alım yönetimi, kamera kayıt sistemi, müşteri ve potansiyel müşteri yönetimi),

* Ekonomik ve finansal veriler (ör. bordro yönetimi, müşteri ve potansiyel müşteri yönetimi),
* Kimlik tespiti verileri (ör. tedarikçi yönetimi, ticari olmayan iletişim, anket ve form, müşteri ve potansiyel müşteri yönetimi),
* Teknik veriler (ör. BT ve telefon yönetimi, yaka kartı yönetimi, çalışan kayıt yönetimi),
* Etkileşimsel veriler (ör. kurumsal yönetim ve tüzel kişilik yönetimi).

Maddi kapsam, işbu BCR-C dokümanı kapsamında ayrıntılı bir Veri İşleme Amaçları ve İlgili Kişi ve Kişisel Veri kategorileri tablosu sunan **Ek 11-A**’da daha kesin olarak detaylandırılmıştır. **Ek 01**, Kişisel Verilerin aktarıldığı üçüncü ülkeler ve BCR Üyeleri hakkında bilgi sağlar.

BCR-C, Kişisel Verileri GDPR’nin uygulama kapsamında yer alan bir BCR Üyesinden BCR-C kapsamında aktarılan tüm İlgili Kişiler için geçerli olacaktır. Bu nedenle BCR Üyesi, BCR-C kapsamının özellikle “AEA vatandaşları veya AEA sakinleri” ile sınırlı olmayabileceğini kabul eder.

Ek olarak işbu BCR-C, söz konusu Kişisel Verilerin kategorisinden ve niteliğinden bağımsız olarak Kişisel Verilerin Veri Sorumlusu olarak hareket eden veya Veri Sorumlusu olarak hareket eden başka bir BCR Üyesi adına Veri İşleyen olarak hareket eden bir BCR Üyesi tarafından işlendiği Veri İşleme durumlarını kapsamaktadır.

Ayrıca her BCR Üyesi, işveren olarak çalışanlarının Kişisel Verilerinin de Veri Sorumlusudur. BCR Üyeleri, kendi çalışanlarının Kişisel Verilerini İşlerken işbu BCR-C hükümlerine riayet edecek ve Kişisel Verileri Çalışan Gizlilik Politikası’nda açıklandığı şekilde işleyecektir.

* 1. Coğrafi kapsam

Concentrix, Kişisel Verilerin işlenmekte olduğu kuruluş bünyesinde mümkün olduğunca tutarlı bir yaklaşım uygulamak istemektedir. Dolayısıyla tüm BCR Üyeleri, konumları veya yasal yargı alanları ne olursa olsun, işbu BCR-C’ye tabidir. Bu nedenle işbu BCR-C, AEA dışındaki BCR Üyelerine aktarılan tüm Kişisel Verileri ve AEA dışındaki diğer BCR Üyelerine yapılan sonraki aktarımları kapsamaktadır. İşbu BCR-C’ye tabi Concentrix kuruluşlarının (bir başka ifadeyle, BCR Üyeleri) Ek 01’de listelendiğini unutmayınız.

Prensip olarak, Concentrix kuruluşları tarafından işbu BCR-C’ye tabi olmayan bir Concentrix kuruluşuna BCR-C’ye tabi olmadıkça veya tabi olana kadar hiçbir Kişisel Veri Aktarımı gerçekleştirilmeyecektir. Bu Concentrix iştiraki, Veri İşleme ve buna bağlı yükümlülüklerin işbu BCR-C’nin gerekliliklerini karşılayacağı ve İlgili Kişilerin haklarının korunmasını sağlayacağı şekilde uygun teknik ve organizasyonel önlemleri uygulamak için yeterli garantiyi sağlamadığı sürece bu tür bir Veri Aktarımı gerçekleştirilemez.

BCR-C’ye tabi BCR Üyesi ve tabi olmayan Concentrix kuruluşları, bunu garanti etmek için yazılı bir anlaşma yapacaktır.

1. Bağlayıcı Mahiyet
   1. Concentrix çalışanları üzerinde

Her BCR Üyesinin çalışanı, İlgili Kişi olarak, işbu BCR-C hükümlerinden yararlanacaktır. Kişisel Verilerin korunması bireysel ve kurumsal bir taahhüt meselesi olduğundan, her çalışan işbu BCR-C kapsamında belirtilen gerekliliklere de uymalıdır.

Bu nedenle BCR-C, Concentrix çalışanlarının iş sözleşmelerinin bir parçası olarak uymaları gereken politikalar kümesine girer. İşbu BCR-C ilkelerine ve kurallarına uyulmaması, iş akdinin feshiyle sonuçlanabilecek disiplin cezalarına ve belirli durumlarda cezai suçlamalara yol açabilir.

* 1. Concentrix Grubunun BCR Üyeleri üzerinde

Bir grup olarak Concentrix, gruba ait tüm BCR Üyelerinin işbu BCR-C kapsamında belirtilen ilke ve yükümlülüklere aynı veya benzer şekilde tabi olmasını ve burada belirtilen gerekliliklere uymasını sağlamak ister.

Bu nedenle işbu BCR-C, tüm BCR Üyeleri için bu BCR-C dokümanını bir ek olarak içeren Grup İçi Veri Aktarım Sözleşmesinin imzalanmasıyla birlikte bağlayıcıdır.

İşbu BCR-C’ye tabi Concentrix kuruluşları listesi, BCR-C’nin Ek 1’inde belirtilmiştir. Lider Avrupa Kuruluşu olarak Webhelp SAS, Grup Veri Koruma Görevlisinin (DPO) yardımıyla, bu listeyi güncel ve erişilebilir tutmayı ve zaman zaman belirlenen şekilde ilgili taraflara talep üzerine iletmeyi taahhüt eder.

* 1. Concentrix Veri İşleyenlerine karşı

Bir BCR Üyesi belirli Veri İşleme faaliyetlerini yürütmek üzere bir Veri İşleyen (ister bir BCR Üyesi, ister BCR’ye henüz tabi olmayan bir Concentrix Grubu iştiraki veya üçüncü taraf bir sağlayıcı) tutarsa söz konusu Veri İşleyen, Veri İşlemenin işbu BCR-P’nin gerekliliklerini karşılayacak şekilde uygun teknik ve organizasyonel önlemlerin uygulanması için yeterli garantiyi sağlayacaktır.

Bu nedenle BCR Üyesinin Veri İşleyenleri tarafından üstlenilen herhangi bir Veri İşleme faaliyeti yazılı bir sözleşme veya diğer bağlayıcı hukuki işlem ile yönetilecek ve aşağıda hatırlatıldığı gibi GDPR Madde 28’in tüm unsurlarını ve özellikle Veri İşlemenin konusunu ve süresini, niteliğini ve amacını, Kişisel Verilerin türünü ve İlgili Kişi kategorilerini ve Veri Sorumlusu olarak hareket eden BCR Üyesinin hak ve yükümlülüklerini belirleyecektir.

Ayrıca bir Veri İşleyen ile yapılan bu sözleşme veya diğer bağlayıcı yasal işlem, aşağıdaki hükümleri düzenleyecektir:

1. Veri İşleyen tabi olduğu Birlik veya Üye Devlet yasaları tarafından zorunlu kılınmadığı sürece Kişisel Verileri yalnızca Veri Sorumlusunun Kişisel Veri Aktarımları ile ilgili olanlar dahil belgelendirilmiş talimatları doğrultusunda işleyecektir (Böyle bir durumda Veri İşleyen, söz konusu yasa bu tür bilgileri kamu yararı açısından önemli gerekçelerle yasaklamadığı sürece veri işleme öncesinde Veri Sorumlusunu bu yasal gereklilik konusunda bilgilendirecektir).
2. Veri İşleyen, özellikle Kişisel Verileri İşlemeye yetkili kişilerin gizliliğe bağlı kalmalarını veya uygun bir yasal gizlilik yükümlülüğü altında olmalarını sağlayarak Kişisel Verileri gizli tutacaktır.
3. Veri İşleyen, Kişisel Verileri korumak için uygun bir güvenlik seviyesi sağlamak üzere uygun teknik, fiziksel ve organizasyonel güvenlik önlemlerini alacaktır.
4. Veri İşleyen, BCR Üyesinin önceden yazılı izni olmadan BCR Üyesine olan yükümlülüğüyle bağlantılı olarak Alt Veri İşleyenin Kişisel Verileri İşlemesine izin vermeyecek ve bu Alt Veri İşleyenin, Veri İşleyen ile BCR Üyesi arasında Birlik veya Üye Devlet yasaları kapsamında bir sözleşme veya diğer yasal işlem yoluyla akdedilen bağlayıcı işlemde belirtilen aynı yükümlülüklere uymayı taahhüt etmesini sağlayacaktır. Alt Veri İşleyenin veri koruma yükümlülüklerini yerine getirememesi durumunda, ilk Veri İşleyen diğer Veri İşleyen yükümlülüklerinin yerine getirilmesi için BCR Üyesine karşı tam olarak sorumlu olmaya devam edecektir.
5. Veri İşleyen, İlgili Kişilerin haklarına ilişkin taleplerinin ele alınması konusunda BCR Üyesine gerekli tüm desteği sağlayacaktır.
6. Veri İşleyen, BCR Üyesine aşağıdaki amaçlar için tüm makul yardımı sağlayacaktır:
   * Veri İşlemenin riske uygun güvenlik düzeyini sağlamak,
   * Kişisel Verileri içeren fiili veya şüpheli herhangi bir güvenlik ihlali konusunda BCR Üyesini fazla gecikmeden bilgilendirmek ve BCR Üyesine, duruma göre, ilgili Denetim Kurumuna bildirimde bulunma ve etkilenen İlgili Kişilerle iletişim kurma konusunda destek sağlamak,
   * Veri koruma etki değerlendirmesi (DPIA) yapmak ve ilgili durumlarda DPIA'nın riski hafifletmeye yönelik önlemlerin yokluğunda yüksek bir riskle sonuçlanması durumunda Denetim Kurumu ile önceden istişare etmek.
7. Veri İşleyen, sözleşmenin veya diğer hukuki bağlayıcı işlemin sona ermesinde kişisel verilerin silinmesi veya iadesi ile ilgili BCR Üyesinin talimatlarına uyacak ve Birlik veya Üye Devlet yasaları Kişisel Verilerin saklanmasını gerektirmediği sürece mevcut kopyaları silecektir.
8. Veri İşleyen, mevzuata uyum sağladığını göstermek ve BCR Üyesi veya BCR Üyesi tarafından yetkilendirilen diğer ilgili kurum veya denetçi tarafından yapılan denetim ve incelemelere katkıda bulunmak için gerekli tüm bilgileri BCR Üyesine sağlayacaktır.
9. Veri İşleyen, bir talimatın işbu BCR-C’yi veya ilgili Geçerli Veri Koruma Mevzuatını ihlal ettiği kanaatine varırsa BCR Üyesini derhal bilgilendirecektir.
10. Kişisel verilerin işlenmesine ilişkin ilkeler

Geçerli Veri Koruma Mevzuatı, Kişisel Verilerin işlenmesi sırasında uyulması gereken bir dizi ilke tanımlar. Concentrix, Veri Sorumlusu veya Veri İşleyen olarak hareket eden bir BCR Üyesi adına bu ilkelere uymayı taahhüt eder.

* 1. Veri İşleme için yasal bir dayanak tanımlama (Şeffaflık, adalet ve yasaya uygunluk)

Kişisel Veriler İşlenirken söz konusu Veri İşlemenin yasal İşleme faaliyetine izin veren temel olan GDPR Madde 6’da sağlananlar gibi uygun bir yasal dayanağı olması gerekir. BCR Üyeleri, aşağıdaki yasal dayanaklardan birinin Kişisel Verilerin İşlenmesi için geçerli olabileceğini kabul eder:

* İlgili Kişilerin onayı,
* İlgili Kişinin taraf olduğu bir sözleşmenin ifası veya böyle bir sözleşme yapılması,
* Veri Sorumlusunun tabi olduğu Birlik veya Üye Devlet yasaları uyarınca belirlenen yasal yükümlülük,
* İlgili Kişilerin veya başka bir bireyin hayati çıkarı,
* Bir görevin kamu yararına veya Veri Sorumlusuna verilen resmi yetkinin kullanılması amacıyla ifası,
* Veri Sorumlusunun veya üçüncü bir tarafın meşru menfaati (söz konusu menfaatin İlgili Kişilerin hak ve özgürlüklerini geçersiz kılmaması kaydıyla).
* Diğer

Bu bağlamda BCR Üyeleri, yalnızca Geçerli Veri Koruma Mevzuatının gerekliliklerine uygun olarak bunu yapmak için geçerli bir yasal dayanağının olduğu durumlarda Kişisel Verileri yasal olarak İşlemeyi taahhüt eder.

Örneğin; Concentrix çalışanlarının Kişisel Verilerinin İşlenmesi çalışanların izin taleplerinin (ör. tatiller) yönetilmesi için gereklidir. Dolayısıyla söz konusu işleme faaliyetinin yasal dayanağı, Concentrix ve çalışanlarının yaptığı istihdam sözleşmesini yürütme zorunluluğudur.

Ayrıca aşağıdaki Madde 5 doğrultusunda BCR Üyeleri şunları sağlamayı taahhüt eder:

* Özel Kişisel Veri Kategorileri yalnızca GDPR Madde 9(2) ile öngörülen muafiyetlerden birine uygun olarak işlenebilir ve
* Cezai hükümler ve suçlarla ilgili Kişisel Verilerin İşlenmesi, GDPR Madde 10 ile öngörülen aynı muafiyetler uygulanmadığı sürece yasaktır.
  1. Bir amacın tanımlanması (Amaç sınırlaması)

Geçerli Veri Koruma Mevzuatı ile özel olarak yetkilendirilmediği sürece BCR Üyeleri, Kişisel Verilerin herhangi bir şekilde toplanması veya İşlenmesinden önce yasal, adil, açık ve meşru bir amaç tespit ettiğinden emin olmalıdır.

BCR Üyeleri, tanımladıkları amaçların Geçerli Veri Koruma Mevzuatını ihlal etmemesini ve meşru görünmesini sağlamayı taahhüt eder ve Kişisel Verilerin bu amaçlarla uyumsuz bir şekilde daha fazla İşlenmemesini temin eder.

Örneğin; hizmetlerini sunmak için gerekli iş gücünün planlanması ve dolayısıyla Concentrix çalışanlarının programlarının yönetilmesi, Çalışanların izin taleplerine ilişkin kişisel verilerinin toplanması için tanımlanan amaçlardan biridir.

* 1. Kişisel Veri toplamanın en aza indirilmesi (Verilerin asgariye indirilmesi)

BCR Üyeleri, Kişisel Verileri İşlendiği amaçlarla ilgili olarak kesinlikle yeterli, ilgili ve gerekli olanla sınırlı olmak üzere toplamayı ve işlemeyi taahhüt eder.

Kişisel Veriler, daha fazla tanımlanmayan bir amaç çerçevesinde büyük ölçüde toplanmayacaktır.

Örneğin; izin talebinin yönetilmesi için toplanan Kişisel Veriler, iznin niteliğiyle (ör. tatiller, doğum izni vs.) ve diğer ilgili bilgilerle (ör. iznin süresi) sınırlıdır ancak kesinlikle gerekli olmayan (çalışanın tatile kiminle gittiği, çalışanın tatil yeri veya hastalık izinleri için herhangi bir sağlık verisi gibi) hiçbir Kişisel Veriyi içermez.

* 1. Kayıt tutma

BCR Üyeleri, bir Veri Sorumlusu veya Veri İşleyen olarak hareket ederken BCR-C’ye uyumu göstermek amacıyla sorumluluğu altındaki tüm Kişisel Veri kategorilerinin İşlenme faaliyetlerinin bir kaydını tutacaktır.

Veri Sorumlusu olarak hareket edildiğinde Veri İşleme Faaliyetlerinin Kaydı, GDPR Madde 30.1 uyarınca en azından aşağıdaki bilgileri içermelidir:

* Concentrix kuruluşunun, potansiyel ortak veri sorumlusunun ve Veri Koruma Görevlisinin adı ve iletişim bilgileri,
* Veri işleme amaçları,
* İlgili Kişiler ve Kişisel Veri kategorilerinin açıklaması,
* Kişisel Veri alıcılarının kategorileri,
* Üçüncü bir ülkeye veya uluslararası bir kuruluşa potansiyel Kişisel Veri aktarımları,
* Veri saklama süresi,
* Veri İşleme riskine uygun bir güvenlik seviyesi sağlamak için gerekli teknik ve organizasyonel güvenlik önlemlerinin genel bir açıklaması.

Örneğin; çalışanların izin taleplerinin yönetilmesi için Veri İşleme faaliyeti, yukarıda listelenen bilgileri içeren çalışan idari yönetimiyle ilgili Veri İşleme Faaliyetleri Kaydına dahil edilmiştir.

Veri İşleyen olarak hareket edildiğinde Veri İşleme Faaliyetlerinin Kaydı, GDPR Madde 30.2 uyarınca en azından aşağıdaki bilgileri içermelidir:

* Veri İşleyen(ler)in ve veri işleyenin adına hareket eden her Veri Sorumlusunun ve uygun hallerde Veri Sorumlusu veya Veri İşleyenin temsilcisinin ve DPO’nun adı ve iletişim bilgileri; Her Veri Sorumlusu adına gerçekleştirilen Veri İşleme kategorileri,
* Uygun hallerde, GDPR Madde 49 uyarınca geçerli uygun güvenlik önlemleri veya muafiyetler kapsamında Kişisel Verilerin üçüncü bir ülkeye Aktarımları.
  1. Kişisel Verilerin Doğruluğu (Veri Doğruluğu)

BCR Üyeleri, topladığı ve işlediği Kişisel Verilerin doğru kalmasını ve gerektiğinde güncel tutulmasını sağlamak için yeterli önlemleri ve kontrolleri uygulayacaktır. Bu amaçla BCR Üyeleri, İşlendiği amaçlar göz önüne alındığında, doğru olmayan Kişisel Verilerin silinmesini veya düzeltilmesini sağlayacak her makul adımı atmak üzere gerekli aksiyonları almayı taahhüt eder.

Örneğin; Çalışanların kişisel durumlarına ilişkin herhangi bir güncellemeyi (ör. adres değişikliği) İK departmanına bildirme görevi vardır. BCR Üyeleri daha sonra Kişisel Verilerin Çalışanların kaydında buna göre güncellenmesini sağlayacaktır.

* 1. Veri saklama süresinin tanımlanması (Sınırlı saklama süresi)

BCR Üyeleri, Kişisel Verileri verilerin toplanma amacı dikkate alındığında kesinlikle gerekenden daha uzun bir süre saklamayacaktır. Bu bağlamda BCR Üyeleri, her Veri İşleme uygulamasından önce bir veri saklama süresi belirlemeyi taahhüt eder.

BCR Üyeleri, bu gerekliliğe uymak için bir veri saklama prosedürü uygulayacak ve belirli bir Veri İşleme faaliyeti ile ilgili olarak uygulanacak yönergeleri belirtecektir.

Örneğin; izin talebinin yönetilmesi amacıyla toplanan Kişisel Veriler; programları yönetmek, bordro ile ilgili işlemleri gerçekleştirmek (ör. ücretsiz izin) ve geçerli yerel zamanaşımı ve muhasebe yükümlülüklerine uymak için gerekli olduğu kadar uzun bir süre için saklanır.

* 1. Güvenlik önlemlerinin uygulanması (bütünlük ve gizlilik)

BCR Üyeleri, hukuka aykırı olarak Kişisel Verilere erişilmemesini ve/veya Kişisel Verilerin İşlenmemesini sağlamak için uygun teknik, fiziksel ve idari önlem ve kontrolleri uygulamıştır. Söz konusu teknik, fiziksel ve idari önlemler bir BCR Üyesi veya Veri İşleyen tarafından iletilen, saklanan veya başka bir şekilde İşlenen Kişisel Verilerin kazara veya kanuna aykırı bir şekilde imhası, kaybedilmesi, değiştirilmesi, izinsiz olarak ifşa edilmesi veya bunlara izinsiz erişilmesi dahil ancak bunlarla sınırlı olmayan riske uygun bir güvenlik düzeyi sağlayacaktır.

Ayrıca BCR Üyeleri, alt yüklenicilerinin / Veri İşleyenlerin GDPR Madde 28.3’te belirtilen gereklilikleri içeren yazılı anlaşmalar yaparak Concentrix'te uygulanan teknik ve organizasyonel güvenlik önlemlerine uymasını sağlar (bkz. yukarıda BCR-C Madde 3.3).

Örneğin, BCR Üyeleri bir Bilgi Güvenliği Politikası (BCR-C Ek 10) hazırlamış ve uygulamıştır. Yerel olarak ise BCR Üyeleri daha özel güvenlik politikaları da uygulamış olabilir. Alt yükleniciler / Veri İşleyenlerle bir anlaşma yaparken BCR Üyeleri sözleşme tarafının Kişisel Verilerin İşlenmesine sağladığı güvenlik düzeyini değerlendirme hakkını saklı tutar.

* 1. Veri Koruma Etki Değerlendirmesi

Veri Koruma Etki Değerlendirmesi (DPIA), Genel Veri Koruma Yönetmeliği ile getirilen ve Veri Sorumlusunun Kişisel Veri İşlemeyi tanımlamasına, gerekliliğini ve orantılılığını kanıtlamasına ve Kişisel Verilerin İşlenmesinden kaynaklanan gerçek kişilerin hak ve özgürlüklerine yönelik riskleri değerlendirerek ve bunları ele almak için önlemler belirleyerek yönetmesine olanak tanıyan risk temelli bir süreçtir. BCR Üyeleri, **Ek 09 Veri Koruma Etki Değerlendirmesi Prosedürü** uyarınca bu etki değerlendirmelerini yapmayı taahhüt eder.

Özellikle yeni teknolojilerin kullanımını içeren bir İşleme türünün İlgili Kişilerin hak ve özgürlükleri için yüksek bir Risk oluşturması muhtemel olduğunda, BCR Üyeleri veri işlemenin niteliğini, kapsamını, bağlamını ve amaçlarını dikkate alarak veri işlemeden önce bir Veri Koruma Etki Değerlendirmesi yapacaktır. Bu gereklilik, veri işleme faaliyetinin değiştirilmesinin beklendiği ve bu değişikliğin İlgili Kişilerin hak ve özgürlükleri için yüksek bir Risk oluşturabileceği mevcut Veri İşleme faaliyetleri için de geçerli olacaktır.

Aşağıdaki durumlardan iki veya daha fazlası doğruysa veri işleme, bir Veri Koruma Etki Değerlendirmesi gerektirecektir:

* Veri İşleme, profilleme ve öngörme dahil olmak üzere gerçek kişilerle ilgili kişisel yönlerin sistematik değerlendirmesini veya puanlamasını içeriyorsa;
* Veri işleme, gerçek kişiyi önemli ölçüde etkileyen otomatik işlemeye dayanıyorsa;
* Veri işleme, hassas Veriler veya son derece kişisel nitelikteki Veriler üzerinde yapılıyorsa;
* Veriler büyük ölçekte işleniyorsa;
* Veri işleme, iki veya daha fazla Veri işleme faaliyetini birleştiriyor veya eşleştiriyorsa;
* Veri işleme, kamuya açık bir alanın sistematik olarak izlenmesini içeriyorsa;
* Veri işleme, savunmasız kişilerin veya çocukların Verileri üzerinde yapılıyorsa;
* eri işleme, yenilikçi kullanım veya uygulama ya da teknolojik veya organizasyonel çözümler içeriyorsa;
* Veri işleme, Verilerin toplandığı amaçlardan farklı amaçlar için yapılıyorsa;
* Veri işleme, İlgili kişilerin haklarını kullanmasını veya bir hizmeti veya sözleşmeyi kullanmasını engelliyorsa.

Ayrıca BCR Üyeleri, ilgili AEA Denetim Kurumunun bir DPIA gerektiren veri işleme faaliyetleri listesi kararına uygun olarak bir DPIA gerektiren İşleme faaliyetleri için bir DPIA yürütecektir.

Bir DPIA, Veri Sorumlusu tarafından riski hafifletmek için alınan önlemlerin yokluğunda Veri İşlemenin yüksek bir Riskle sonuçlanacağını gösterdiğinde ve bir DPIA yüksek artık Riskler ortaya koyduğunda, BCR Üyesi bu Veri İşlemeyi gerçekleştirmeden önce AEA Denetim Kurumuna önceden danışacaktır.

Örneğin; çalışanların izin talebinin yönetilmesi, İlgili Kişilerin hak ve özgürlükleri için yüksek risk oluşturduğu düşünülen bir işlem değildir. Yine de bir BCR Üyesi yukarıda listelenen kriterlerden ikisini veya daha fazlasını karşılayan bir veri işleme tespit ettiğinde Ek 9'da daha ayrıntılı olarak açıklanan prosedüre uygun olarak DPO gözetiminde bir DPIA gerçekleştirilir.

* 1. Concentrix Grubu Dışındaki Alt Veri İşleme ve Veri Aktarımları

BCR Üyeleri, BCR Üyesi olmayan Veri Sorumlularına ve/veya Veri İşleyenlere, bu Veri Sorumluları ve/veya Veri İşleyenleri yeterli garanti sağlamadığı ve BCR-C'de sağlananlar gibi uygun teknik ve organizasyonel önlemleri, Veri İşlemenin işbu BCR-C'nin gerekliliklerini karşılayacak şekilde uygulamadığı sürece hiçbir Kişisel Veri Aktarımı yapmamayı taahhüt eder.

Bu bağlamda BCR Üyeleri, hukuka aykırı olarak Kişisel Verilere erişim sağlanmamasını ve/veya Kişisel Verilerin İşlenmemesini sağlamak ve kontrol etmek için uygun teknik, fiziksel ve idari önlemler uygulamıştır.

Herhangi bir BCR Üyesinin, Kişisel Verileri İşliyorlarsa Concentrix Grubu dışındaki (veya BCR-C'ye tabi olmayan) bir Veri Sorumlusu veya Veri İşleyen ile yazılı bir sözleşme veya diğer bağlayıcı yasal işlem yapması gerekir. Yukarıda belirtilen sözleşme veya diğer bağlayıcı yasal işlem, Madde 3.3'te belirtilen unsurları belirleyecektir. Söz konusu sözleşme işbu BCR-C’yi içerebilir.

Bu nedenle başka bir BCR Üyesi adına Veri Sorumlusu veya Veri İşleyen olarak hareket eden bir BCR Üyesi, AEA dışında kurulmuş olan bir alt yüklenicinin hizmetlerini kullanıyorsa ve gerçekleştirilen hizmetlerin Amacı için çalışanlarının Kişisel Verilerini paylaşması gerekiyorsa (sadece operasyonlar için gerekli ölçüde) BCR Üyesi, Veri Aktarımından önce alt yüklenicinin BCR-C gerekliliklerini karşılayabileceğini değerlendirecek ve Veri Aktarımını uygun bağlayıcı yasal işlemle güvence altına alacaktır.

* 1. Kişisel Veri İhlali bildirim önlemlerinin uygulanması

Bir Kişisel Veri İhlali meydana geldiğinde BCR Üyeleri, Concentrix tarafından benimsenen geçerli Veri İhlali prosedürüne uyacaktır.

Her halükarda BCR Üyeleri, Kişisel Veri İhlalini fazla gecikmeden ve mümkün olduğu takdirde farkına vardıktan sonra en geç 72 saat içinde (1) Webhelp SAS'a (Sorumlu BCR Üyesi olarak) ve Veri Sorumlusu olarak hareket ediyorlarsa diğer ilgili Yerel Gizlilik Liderlerine ve veri işleyen olarak hareket ediyorlarsa Veri Sorumlusu olarak hareket eden BCR Üyesine (2) Kişisel Veri İhlalinin gerçek kişilerin hak ve özgürlükleri için bir risk oluşturması muhtemel değilse yetkili AEA Denetim Kurumuna bildirecektir.

Yukarıda bahsedilen bildirim en azından aşağıdaki bilgileri kapsayacaktır:

* Kişisel Veri İhlalinin niteliği ve kapsamı, mümkün olduğunda ilgili Veri Sahiplerinin kategorileri ve yaklaşık sayısı ile ilgili Kişisel Veri kayıtlarının kategorileri ve yaklaşık sayısı dahil,
* (Grup) Veri Koruma Görevlisinin (“**DPO**") veya daha fazla bilgi edinilebilecek diğer irtibat kişisinin adı ve iletişim bilgileri,
* Kişisel Veri ihlalinin muhtemel sonuçlarının belirtilmesi,
* gerekli durumlarda olası olumsuz etkileri hafifletecek önlemler de dâhil olmak üzere Veri Sorumlusunun Kişisel Veri ihlalini gidermek için aldığı veya alınmasını önerdiği önlemlerin belirtilmesi.

Herhangi bir BCR Üyesinin, Kişisel Verileri Veri Sorumlusu olarak kendi adına işlerken ve Veri Sorumlusu olarak hareket eden başka bir BCR Üyesi adına işlerken GDPR Madde 34 uyarınca Kişisel Veri İhlalinin gerçek kişilerin hakları ve özgürlükleri için yüksek bir risk oluşturması muhtemel olduğu durumlarda söz konusu Kişisel Veri İhlalini İlgili Kişilere de iletmesi gerekebilir. Bu gibi durumlarda, kişisel veri ihlali gecikmeksizin bildirilecek ve yetkili AEA Denetim Kurumuna iletilecek olan yukarıda belirtilen unsurları da kapsayacaktır.

BCR Üyeleri, herhangi bir Kişisel Veri İhlalini ve yukarıda belirtilen bilgileri belgelendirecektir. BCR Üyeleri, talep edilmesi halinde bu belgeleri Yetkili AEA Denetim Kurumuna sunacaktır.

İletilen, saklanan veya başka bir şekilde işlenen Kişisel Verilerin kazara veya kanuna aykırı bir şekilde imhası, kaybedilmesi, değiştirilmesi, izinsiz olarak ifşa edilmesi veya bunlara izinsiz erişilmesine yol açan bir güvenlik ihlali durumunda, BCR Üyeleri **Ek 08 Kişisel Veri İhlali Bildirimi Prosedürü**'nde açıklanan Kişisel İhlal prosedürüne uygun şekilde ilerleyecektir.

1. Hassas verilerin işlenmesi

BCR Üyeleri, Madde 4 – Kişisel Verilerin İşlenmesine İlişkin İlkelerin hükümlerine uymayı taahhüt eder ve Hassas Kişisel Veriler, İlgili Kişilerin temel hak ve özgürlükleri ile ilgili önemli riskler oluşturabileceğinden Hassas Kişisel Verilerin özel bir koruma uygulanmasını gerektirdiğini kabul eder.

BCR Üyeleri, Hassas Kişisel Verileri Geçerli Veri Koruma Mevzuatı ve uygun yerlerde AEA Denetim Kurumları tarafından benimsenen diğer sektörel çerçeveye uygun olarak işlemeyi taahhüt eder.

Söz konusu Veri İşleme, özellikle Concentrix çalışanları ile ilgili olarak sınırlı ve özel olacaktır.

BCR Üyeleri, Hassas Kişisel Verileri kendi adına işlemeyi amaçladığında şu hususları sağlayacaktır:

* Veri İşlemenin gerekli ve yasal olması,
* Veri İşlemenin uygun güvenlik önlemleri ve kontrollerle gerçekleştirilmesi,
* Gerektiğinde İlgili Kişinin bu Hassas Kişisel Verilerin bir veya daha fazla belirtilen amaç için İşlenmesine açık rıza vermiş olması. Söz konusu onay, (1) İlgili Kişinin onay verme konumunda olmaması ve Veri İşlemenin İlgili Kişinin veya başka bir kişinin hayati çıkarlarını korumak için gerekli olması durumunda, (2) İlgili Kişinin kendisinin etkilenen Hassas Kişisel Verileri zaten açıkça kamu malı haline getirmiş olması durumunda, (3) Uygulanabilir olduğunda Veri İşlemenin Geçerli Veri Koruma Mevzuatı veya herhangi bir ulusal yasa (ör. azınlıkların kaydı/korunması) tarafından açıkça izin verilmiş olması durumunda gerekli olarak kabul edilmeyecektir.
* İlgili Kişinin söz konusu verilerin İşlenmemesini sağlama konusunda üstün bir meşru çıkarı olduğunu varsaymak için hiçbir gerekçe olmaması koşuluyla, gerektiğinde Veri İşlemenin yasal iddiaları oluşturma, kullanma veya savunma amacıyla zorunlu olması.

1. Kişisel Verilerin üçüncü ülkelere aktarılması ve BCR Üyesi Olmayanlara ileriye dönük Aktarım kısıtlaması
   1. Kişisel Veri Aktarımları ve ileriye dönük Aktarımlar

BCR Üyeleri, faaliyetleri sırasında Kişisel Verileri Concentrix Grubu’nun diğer kuruluşlarına (BCR Üyesi olsun veya olmasın) veya üçüncü taraflara aktarabilir. Söz konusu Concentrix kuruluşları veya üçüncü taraflar, Avrupa Ekonomik Alanı (bundan böyle “**AEA**”) dışında bulunabilir. Böyle bir durumda, Kişisel Verilerin Aktarımının gerçekleşeceği kabul edilir.

Kişisel Veriler Aktarıldığında Concentrix, aktarılan Kişisel Verilerin aşağıda daha ayrıntılı olarak açıklandığı gibi yeterli bir koruma seviyesinden yararlanmasını sağlamak için belirli garantiler uygulayacaktır:

* Veri Sorumlusu olarak hareket eden bir BCR Üyesinden, AEA dışında bulunan ve Veri Sorumlusu veya Veri İşleyen olarak hareket eden başka bir BCR Üyesine yapılan Kişisel Veri Aktarımları, işbu BCR-C’nin hükümleri ile desteklenecektir.
* Veri Sorumlusu olarak hareket eden bir BCR Üyesinden, AEA dışında bulunan (daha spesifik olarak AB Komisyonu tarafından yeterlilik kararı verilmiş bir AEA dışı ülkeye) ve Veri İşleyen olarak hareket eden ya (BCR Üyesi olmayan) bir Concentrix kuruluşuna ya da üçüncü taraflara yapılan Kişisel Veri Aktarımları, yetkili AEA Denetim Kurumu ve/veya AB Komisyonu tarafından kabul edilen (AB Komisyonu Aktarımlar Hakkındaki SCC’ler (914/2021), Modül 2 Veri Sorumlusundan Veri İşleyene gibi) geçerli standart sözleşme maddelerini içeren yazılı bir anlaşma ile desteklenecektir.
* Veri Sorumlusu olarak hareket eden bir BCR Üyesinden, AEA dışında bulunan (daha spesifik olarak AB Komisyonu tarafından yeterlilik kararı verilmiş bir AEA dışı ülkeye) ve Veri Sorumlusu olarak hareket eden ya (BCR Üyesi olmayan) bir Concentrix kuruluşuna ya da üçüncü taraflara yapılan Kişisel Veri Aktarımları, yetkili AEA Denetim Kurumu ve/veya AB Komisyonu tarafından kabul edilen (AB Komisyonu Aktarımlar Hakkındaki SCC’ler (914/2021), Modül 1 Veri Sorumlusundan Veri Sorumlusuna gibi) geçerli standart sözleşme maddelerini içeren yazılı bir anlaşma ile desteklenecektir.
* Yukarıda açıklandığı gibi bir yeterlilik kararı veya uygun güvenlik önlemlerinin bulunmaması durumunda, GDPR Madde 49 uyarınca bir istisna geçerliyse ve ilgili durumlar ara sıra olacak ve tekrarlamayacak şekilde Veri Aktarımları istisnai olarak gerçekleşebilir.

Her halükarda BCR Üyeleri, öncelikle GDRP ile güvence altına alınan İlgili Kişilerin koruma düzeyinin zayıflatılmamasını sağlamak için aktarılan Kişisel Verilere GDRP ile sağlanan korumayla uyumlu yeterli bir koruma düzeyinin sağlanacağından emin olmadan Kişisel Verileri Concentrix Grubunun bir parçası olmayan üçüncü taraflara (veya BCR Üyesi olmayan bir Concentrix kuruluşuna) aktarmamayı taahhüt eder.

Daha spesifik olarak BCR Üyeleri, BCR-C kapsamında iki BCR Üyesi arasında aktarılan Kişisel Verilerin, yalnızca GDPR Madde 44 ila 46’da belirtilen ve burada yansıtılan Veri Aktarımlarına ilişkin gerekliliklerin sağlanması koşuluyla, AEA dışına BCR-C'ye tabi olmayan Veri İşleyenlere ve Sorumlularına aktarılabileceğini kabul eder.

* 1. Devletin erişim talebi durumunda Veri Alıcısının yükümlülüğü

Veri Alıcısı olarak hareket eden BCR Üyesinin, Veri Sağlayıcısına BCR-C (aşağıda Madde 12.3) kapsamındaki taahhütlere uyma konusundaki yetersizliğini bildirme yükümlülüğü saklı kalmak üzere Veri Alıcısı olarak hareket eden BCR Üyesi, aşağıdaki durumlarda Veri Sağlayıcısını ve mümkünse İlgili Kişiyi (gerekirse Veri Sağlayıcısının yardımıyla) derhal bilgilendirecektir:

* Hedef ülkenin veya diğer bir üçüncü ülkenin yasaları uyarınca bir resmi kurumdan BCR-C uyarınca aktarılan Kişisel Verilerin ifşası için yasal olarak bağlayıcı bir talep alırsa. Söz konusu bildirim; talep edilen Kişisel Veriler, talep eden kurum, talebin yasal dayanağı ve verilen yanıt hakkında bilgiler içerecektir.
* Hedef ülkenin yasalarına göre BCR-C uyarınca aktarılan Kişisel Verilere resmi kurumların doğrudan erişiminden haberdar olursa. Söz konusu bildirim Veri Alıcısının erişebildiği tüm bilgileri içerecektir.

Veri Sağlayıcısına ve/veya ilgili kişiye bildirimde bulunması yasaklanırsa Veri Alıcısı, mümkün olduğunca fazla bilgiyi en kısa zamanda iletmek üzere bu yasaktan feragat etmek için en iyi çabayı gösterecek ve Veri Sağlayıcısının talebi üzerine gösterebilmek için çabalarını belgeleyecektir.

Veri Alıcısı, Veri Sağlayıcısı olarak hareket eden BCR Üyesine düzenli aralıklarla alınan talepler konusunda mümkün olduğunca fazla bilgi sağlayacaktır (özellikle talep sayısı, talep edilen veri türü, talep eden kurum(lar) taleplere itiraz edilip edilmediği ve bu itirazların sonucu, vs.). Veri Alıcısının Veri Sağlayıcısına yukarıda belirtilen bilgileri kısmen veya tamamen sağlaması yasaklanırsa Veri Alıcısı, Veri Sağlayıcısını uygun şekilde gecikmeden bilgilendirecektir.

Veri Alıcısı yukarıda belirtilen bilgileri, Kişisel Veriler BCR-C ile sağlanan güvencelere tabi olduğu sürece saklayacak ve talep üzerine Yetkili Denetim Kurumuna sunacaktır.

Veri Alıcısı, ifşa talebinin yasallığını, özellikle de talep eden resmi kuruma verilen yetkiler dahilinde kalıp kalmadığını inceleyecek ve dikkatli bir değerlendirmenin ardından talebin hedef ülkenin yasaları, uluslararası hukuk kapsamındaki geçerli yükümlülükler ve uluslararası nezaket ilkeleri uyarınca hukuka aykırı olduğunu düşünmek için makul gerekçeler olduğuna karar verirse bu talebe itiraz edecektir.

Veri Alıcısı, aynı koşullar altında itiraz olanaklarını gözetecektir.

Bir talebe itiraz ederken Veri Alıcısı, yetkili adli kurum talebin esasına karar verene kadar talebin etkilerini askıya almak amacıyla geçici tedbirler arayacaktır. Veri Alıcısı, geçerli usul kuralları uyarınca bunu yapması gerekene kadar talep edilen Kişisel Verileri ifşa etmeyecektir.

Veri Alıcısı, yasal değerlendirmesini ve ifşa talebine yönelik itirazı belgelendirecek ve hedef ülkenin yasaları uyarınca izin verilen ölçüde belgeleri Veri Sağlayıcısına sunacaktır. Veri Alıcısı, talep edilmesi halinde belgeleri Yetkili Denetim Kurumuna da sunacaktır.

Veri Alıcısı, söz konusu talebin makul yorumuna dayanarak ifşa talebine yanıt verirken izin verilen asgari miktarda bilgiyi sağlayacaktır.

Her halükarda bir BCR Üyesi tarafından herhangi bir resmi kuruma yapılan Kişisel Veri Aktarımları demokratik bir toplumda gerekli olanın ötesine geçecek şekilde büyük çapta, orantısız ve gelişigüzel olamaz (bu konu için bkz. BCR-C Madde 12.3).

1. İlgili Kişinin Hakları
   1. Üçüncü Taraf Lehtar Hakları

Ne zaman bir BCR Üyesi, Kişisel Verileri Veri Sorumlusu veya Veri İşleyen olarak kendi adına işlerse **İlgili Kişiler, işbu BCR-C'yi üçüncü taraf lehtar olarak uygulama hakkına sahip olurlar.**

**İlgili Kişiler en azından aşağıdaki unsurları uygulayabilmelidir:**

* Veri işleme için yasal dayanak (Madde 4.1),
* Veri İşlemenin amaç sınırlaması (Madde 4.2),
* Verilerin asgariye indirilmesi (Madde 4.3),
* Saklama sürelerinin sınırlandırılması (Madde 4.6),
* Veri doğruluğu (Madde 4.5),
* Kişisel Verilerin Güvenliği, özellikle
  + Kasten ve varsayılan veri koruması ile veri güvenliğini sağlamaya yönelik önlemler (Madde 12 ve 4.7),
  + Kişisel Veri ihlalinin hak ve özgürlükleri için yüksek risk oluşturması muhtemel olduğunda Kişisel Veri İhlali bildirimi (Madde 4.10),
* Özel Kişisel Veri kategorileri ile cezai hüküm ve suçlarla ilgili Kişisel Verilerin İşlenmesinde belirli kurallar (Madde 5),
* Şeffaflık ve BCR-C’ye kolay erişim (Madde 12.1),
* İleriye dönük veri aktarımları (Madde 4.9),
* Erişim, düzeltme, silme ve kısıtlama hakkı, kişisel verilerin açıklandığı her alıcıya düzeltme, silme veya kısıtlama ile ilgili bildirim hakkı, veri işlemeye itiraz hakkı, veri taşınabilirliği hakkı, profilleme dahil olmak üzere yalnızca otomatik işleme dayalı kararlara tabi olmama hakkı (Madde 7.4 ve 7.5),
* BCR'lere uyulmasını engelleyen ulusal mevzuat (Madde 12.3) ve hükümet erişim talepleri durumu (Madde 6.2),
* Şirketlerin dahili şikayet mekanizması aracılığıyla şikayette bulunma hakkı (BCR Madde 8 ve Ek 5 – Madde 3.1),
* AEA Denetim Kurumu ile iş birliği görevleri (Madde 12.4),
* Yetkili AEA Denetim Kurumuna şikayette bulunma hakkı (daimi ikametgahının, çalışma yerinin veya iddia edilen ihlalin gerçekleştiği yerin bulunduğu Üye Devletteki denetim Kurumuna başvurma seçeneği) ve AB Üye Devletinin yetkili mahkemesine başvurma hakkı (İlgili Kişinin veri sorumlusunun veya veri işleyenin bir kuruluşunun bulunduğu veya İlgili Kişinin daimi ikametgahının bulunduğu mahkemelerde dava açma seçeneği) (Madde 8),
* İlgili Kişileri BCR-C’nin ve işbu BCR-C’ye tabi olan BCR Üyeleri listesinin güncellenmesi konusunda bilgilendirme görevi (Madde 13),
* Mevcut Üçüncü taraf lehtar hakları (Madde 7),
* BCR-C'nin uygulanabilir unsurlarından birinin ihlali durumunda yargı yoluna başvurma hakkı, telafi ve uygun hallerde tazminat alma hakkı (BCR Madde 7 ve 8 ve Ek 5 – Madde 3.4.2).

Bu nedenle BCR Üyeleri, İlgili Kişilerin yukarıda belirtilen BCR-C'nin uygulanabilir unsurlarından birine uyulmaması durumunda, aşağıda tanımlanan koşullar altında yargısal çözüm yolları ve/veya bir veri koruma kurumu nezdinde çözüm yolları arama ve herhangi bir BCR Üyesi tarafından BCR-C'nin ihlalinden kaynaklanan zararlar için tazminat alma hakkına sahip olduğunu kabul eder.

Bir BCR Üyesi, İlgili Kişilerin adına şikayette bulunmak, yukarıda bahsedilen hakları kullanmak için kar amacı gütmeyen bir kuruluş, organizasyon veya dernek tarafından temsil edilebileceğini kabul eder. Söz konusu kuruluş, organizasyon veya dernek, bir Üye Devletin yasalarına uygun şekilde kurulmuş olmalı, kamu yararına yasal amaçlara sahip olmalı ve İlgili Kişilerin Kişisel Verilerinin korunmasına ilişkin hak ve özgürlüklerinin korunması alanında faaliyet göstermelidir.

Anlaşılabilirlik adına, yukarıda açıklanan üçüncü taraf lehtar haklarının eğitim, denetim programı, uyumluluk ağı ve BCR-C güncelleme mekanizması gibi kuruluşlar içinde uygulanan iç mekanizmalara ilişkin BCR-C'nin bu unsurlarına uzanmadığı belirtilmiştir.

**İşbu Madde 7 hükümlerine halel gelmeksizin, Concentrix’in İlgili Kişileri aşağıda BCR Madde 8’de açıklanan dahili şikayet mekanizmasını kullanmaya teşvik ettiğini unutmayın.**

* 1. AEA içindeki bir BCR Üyesinin BCR-C’ye uymaması durumunda şikayette bulunma ve yargısal çözüm, düzeltme ve tazminat alma hakkı

AEA içindeki bir BCR Üyesinin yukarıdaki bir önceki bölüm 7.1’de sayılan BCR-C'nin uygulanabilir unsurlarından birine uymaması halinde Concentrix, uyumsuzluktan sorumlu olan AEA içindeki BCR Üyesinin sorumluluk taşıyacağını ve eylemini düzeltmeye yönelik gerekli aksiyonları alacağını kabul eder.

.

Concentrix, İlgili Kişinin aşağıdaki hususlarda hak sahibi olduğunu da kabul eder:

* Özellikle daimi ikametgahının, iş yerinin veya iddia edilen ihlalin gerçekleştiği yerin bulunduğu Üye Devlette bir AEA Denetim Kurumuna şikayette bulunma ve/veya
* İşbu BCR-C’nin bir BCR Üyesi tarafından Veri Sorumlusu olarak veya bir BCR Üyesi tarafından kendi adına Kişisel Verileri İşleyen bir Veri İşleyen olarak ihlal edildiğini iddia ettiği durumlarda etkili bir yargısal çözüm. Concentrix, söz konusu iddianın BCR-C’ye uyulmamasından sorumlu olan BCR Üyesinin kurulduğu Üye Devletin yetkili mahkemesi nezdinde veya İlgili Kişinin daimi ikametgahının bulunduğu yerin mahkemesinde ileri sürülebileceğini kabul eder.
  1. AEA dışındaki bir BCR Üyesinin BCR-C’ye uymaması durumunda şikayette bulunma ve yargısal çözüm, düzeltme ve tazminat alma hakkı

AEA dışındaki bir BCR Üyesinin yukarıda sayılan BCR-C'nin uygulanabilir unsurlarından birine uymaması halinde Webhelp SAS, Avrupa Lider Kuruluşu olarak (1) “Sorumlu BCR Üyesi” olmayı kabul eder ve bu itibarla yetkili mahkeme tarafından verildiğinde tazminat ödemesi de dahil olmak üzere BCR-C'ye uyulmamasından kaynaklı maddi ve manevi zararların sorumluluğunu üstlenir ve (2) AEA dışındaki diğer BCR Üyesinin eylemlerini düzeltmek için gerekli aksiyonları almayı kabul eder.

.

Bu gibi durumlarda ayrıca Webhelp SAS, AEA dışında bulunan (Veri Sorumlusu veya Veri İşleyen olarak hareket eden) BCR Üyesinin Bölüm 7.1’de sayılan uygulanabilir unsurlardan birini ihlal ettiğini düşünen herhangi bir İlgili Kişinin şu haklara sahip olacağını kabul eder:

* İkametgahı ve iş yerinin bulunduğu veya devredilmiş sorumluluğa sahip BCR Üyesinin kurulduğu yerde bir veri koruma kurumuna şikayette bulunmak ve/veya
* Bu ihlal AEA dışında bulunan BCR Üyesi yerine Webhelp SAS tarafından yapılmış gibi, Webhelp SAS'ın yerleşik olduğu veya İlgili Kişilerin ikamet ettiği veya çalıştığı yerin mahkemeleri veya adli makamları nezdinde etkili bir yargısal çözüm.

İlgili Kişiler zarar gördüğünü gösterebilir ve bu zararın BCR-C’nin ihlali nedeniyle meydana gelmiş olma ihtimalinin yüksek olduğunu kanıtlarsa Webhelp SAS, AEA dışındaki söz konusu BCR üyesinin zararlara yol açan BCR-C ihlalinden sorumlu olmadığını veya böyle bir ihlalin gerçekleşmediğini göstermekten sorumlu olacaktır. Webhelp SAS, AEA dışında bulunan diğer BCR Üyesinin bu fiilden sorumlu olmadığını gösterebilirse kendisini her türlü sorumluluktan kurtarabilir.

* 1. İlgili Kişilerin Hakları

İlgili Kişiler aşağıdaki haklardan yararlanma hakkına sahiptir:

* Kendisiyle ilgili ve bir BCR Üyesi tarafından İşlenen Kişisel Verilere erişim,
* Kendisiyle ilgili yanlış veya eksik Kişisel Veriler ile Veri İşleme amacının artık yasal veya uygun olmadığı Kişisel Verilerin düzeltilmesi veya silinmesi talebi,
* Kendisiyle ilgili Kişisel Veri İşlemenin sınırlandırılmasını talep etme,
* Söz konusu Veri İşlemenin Veri Sorumlusu olarak hareket eden BCR Üyesinin veya üçüncü bir tarafın gözettiği meşru menfaat amaçları için gerekli olması durumunda BCR Üyesinin gözettiği menfaatler, İlgili Kişilerin menfaat hak ve özgürlüklerini geçersiz kılmadığı sürece kendi kişisel durumuyla ilgili gerekçelerle dilediği zaman profilleme dahil meşru menfaat amaçları için Kişisel Verilerinin bir BCR Üyesi tarafından İşlenmesine itiraz etme,
* Kişisel Verilerinin profilleme dahil olmak üzere pazarlama amaçları için İşlenmesine itiraz etme ve
* Kişisel Verilerini yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilen bir biçimde ve İşleme otomatik yollarla gerçekleştirildiğinde birlikte işlem görebilir şekilde alma.

Bir BCR Üyesi, Veri Sorumlusu olarak hareket ettiğinde bu tür bir talebi fazla gecikmeden ve aşağıda Bölüm 8’de belirtilen şikayet işleme prosedürüne uygun olarak ele alacaktır.

Veri Sorumlusu olarak hareket eden BCR Üyesi, İlgili Kişinin talebi üzerine gerçekleştirilen Kişisel Verilerin düzeltilmesi veya silinmesi ya da Veri İşlemenin kısıtlanması durumunu, bunun imkansız olduğu veya orantısız çaba gerektirdiği durumlar hariç olmak üzere, Kişisel Verilerin açıklandığı her alıcıya iletecektir. Ayrıca söz konusu BCR Üyesi, İlgili Kişinin talep etmesi halinde İlgili Kişiye bu alıcılar hakkında bilgi verecektir.

* 1. İlgili Kişilerin Haklarının Kullanılması

İlgili Kişiler, işbu BCR-C'yi üçüncü taraf lehtar olarak uygulama ve Kişisel Verilerinin Veri Sorumlusu olarak hareket eden herhangi bir BCR Üyesi tarafından İşlenmesiyle ilgili haklarını kullanma hakkına sahiptir. BCR Üyesi, İlgili Kişinin haklarının kullanımına ilişkin herhangi bir talebinin veya şikayetinin (“**Talepler**”) zamanında ele alınmasını sağlayacaktır.

İlgili Kişiler sözlü veya yazılı olarak talepte bulunabilir. BCR Üyeleri, İlgili Kişilere haklarını kullanabilecekleri erişilebilir araçlar ve özellikle:

1 - İlgili Kişinin bulunduğu ülkeden bağımsız olarak kullanabileceği tek bir özel iletişim e-postası sağlayacaktır:

[dpo@concentrix.com](mailto:dpo@concentrix.com)

Kullanılan dil gibi yerel özellikleri dikkate almak için yerel e-postalar kullanılabilir.

Yerel gizlilik irtibat kişinize ulaşmak için lütfen Ek 01 - BCR-C’ye tabi Concentrix kuruluşları ve yerel Gizlilik e-posta iletişim listesi dokümanına bakınız.

2 - www.concentrix.com adresinden erişilebilen Concentrix DPO e-posta adresinin bulunduğu tek bir portal

3 - İlgili Kişinin bulunduğu ülkeden bağımsız olarak kullanabileceği tek özel posta adresi:

Group Data Privacy Officer (Grup Veri Koruma Görevlisi)

Legal and Compliance Department (Hukuk ve Mevzuat Uyum Departmanı)

3 rue d’Heliopolis

75017 – PARİS

FRANSA

DPO veya DPO’nun Talepleri yönetmek üzere atadığı, kurum içi veya dışı, herhangi bir diğer kişi veya kuruluş, (i) söz konusu İlgili Kişiden Talebini ele almak için gerekli asgari bilgilerin alınmasını sağlayacak ve (ii) gerekli görüldüğü takdirde, Talebin usulüne uygun şekilde ele alınmasını sağlamak için mümkün olduğunca fazla bilgi edinecektir.

Talepte bulunan kişinin kimliği konusunda şüphe varsa özellikle uzaktan iletişim araçları kullanıldığında, bir BCR Üyesinin İlgili Kişiler hakkında daha fazla bilgi istemesi gerekebilir. Toplanan bilgiler (i) talepte bulunan kişinin kim olduğunu doğrulamak için gerekli olan bilgilerle sınırlı olacak ve (ii) bir BCR Üyesi veya Müşterileri tarafından sağlanan ürün veya hizmetler kullanıcının gerçek kimliği altında teslim edilmediğinde toplanmayacaktır. Orantılılık her zaman Veri Sorumlusu tarafından değerlendirilecektir.

Her durumda, Talebin alınmasından itibaren en geç 1 ay içinde İlgili Kişiye yanıt verilmelidir. Taleplerin karmaşıklığı ve sayısı dikkate alındığında, bu bir aylık süre en fazla iki ay daha uzatılabilir; bu durumda şikayetçi buna göre bilgilendirilmelidir (Ek 5’te ayrıntılı olarak açıklandığı üzere).

İlgili Kişi, BCR Üyesi tarafından sağlanan ilk yanıttan memnun kalmazsa her halükarda Talebinin yeniden incelenmesini derhal talep etme hakkına sahip olacaktır. İlgili Kişi, BCR Üyesine daha önce sağlanan çözümün yeterli olmayan hükümlerine dair ayrıntılı bir açıklama sunacaktır. BCR Üyesi, Talebin alınmasından itibaren en geç 2 ay içinde talebin nasıl ele alınacağını belirlemek için yeniden incelemeyi dikkate alacak ve İlgili Kişiyi bu konuda yazılı olarak bilgilendirecektir.

İlgili Kişinin Talebi veya şikayeti, BCR Üyesi tarafından reddedilir veya verilen yanıt İlgili Kişinin talebini karşılamazsa yukarıda bölüm 7.1 ve 7.2’de daha ayrıntılı olarak açıklandığı üzere İlgili Kişi, DPO ile iletişime geçebilir ve/veya doğrudan yetkili bir AEA Denetim Kurumuna şikayette bulunabilir ve/veya yargı yoluna başvurabilir.

İşbu Madde ile ilgili daha fazla ayrıntı aşağıdaki ekte mevcuttur:

* **Ek 5 - Concentrix’in Veri Sorumlusu olarak hareket ettiği durumlarda İlgili Kişilerin taleplerine ilişkin prosedür**

1. İlgili Kişilerin şikayet yönetimi prosedürü

İlgili Kişiler, işbu BCR-C’ye uygun hareket etmediğini düşündükleri BCR Üyesi nezdinde BCR-C ile uyumlu olmadığını düşündükleri Kişisel Verilerin İşlenmesiyle ilgili olarak doğrudan bir BCR Üyesine şikayette bulunma hakkına sahiptir. Bu ihlalin AEA dışında bulunan bir BCR Üyesinin eyleminden kaynaklanması muhtemel olduğunda İlgili Kişi, doğrudan Avrupa Lider Kuruluşu olarak Webhelp SAS nezdinde bir şikayette bulunabilir.

İlgili Kişiler, şu şekilde şikayette bulunabilir:

1. İlgili BCR Üyesinin Yerel Gizlilik Liderine, BCR-C'nin Ek 01'inde verilen adrese e-posta göndererek ve/veya

Grup Veri Koruma Görevlisine [dpo@concentrix.com](mailto:dpo@concentrix.com) adresinden veya posta yoluyla 3/5 rue d’Heliopolis, 75017, Paris, Fransa adresinden ulaşarak. Bu tür şikayetler, ilgili BCR Üyesi(leri) tarafından uygun zamanda ve burada tanımlanan adımlara ve zamanlamaya göre özel bir özen ve dikkat gösterilerek ele alınacaktır. Bu hükümler, İlgili Kişilerin haklarını kullanma talepleriyle ilgili olarak da geçerlidir (bkz. yukarıda Madde 7).

Uygulamada, İlgili Kişiler tarafından yapılan şikayetler **Ek 5 - Concentrix’in Veri Sorumlusu olarak hareket ettiği durumlarda İlgili Kişilerin taleplerine ilişkin prosedür** kapsamında tanımlanan prosedüre göre ele alınacaktır.

Veri Sorumlusu olarak hareket eden BCR Üyesi, alınan aksiyonlar konusunda İlgili Kişiye / şikayetçiye fazla gecikmeden ve her durumda bu hükümlere uygun olarak şikayetin yapıldığı tarihten itibaren bir ay içinde bilgi sağlayacaktır. Şikayet, işlevlerini yerine getirirken uygun düzeyde bağımsızlığa sahip açıkça tanımlanmış bir departman veya kişi tarafından ele alınacaktır. Uygulamada, ilgili departman veya kişi Hukuk & Mevzuat Uyum departmanı (özellikle ilgili Coğrafi Mevzuat Uyum Görevlisi veya Yerel Gizlilik Lideri) olacaktır. Taleplerin karmaşıklığı ve sayısı dikkate alındığında, bu bir aylık süre en fazla iki ay daha uzatılabilir; bu durumda şikayetçi buna göre bilgilendirilmelidir.

BCR Üyesinin İlgili Kişi tarafından yapılan şikayeti reddetmeye karar vermesi durumunda söz konusu BCR Üyesi, İlgili Kişiye kararını bildirmeyi ve kendisine bunun nedeni hakkında bilgi sağlamayı taahhüt eder.

BCR Üyesi, İlgili Kişi tarafından yapılan şikayetin haklı olduğunu düşünürse makul ölçüde mümkün olan en kısa sürede bu durumu düzeltmek için yeterli gördüğü düzeltici önlemleri uygulamayı taahhüt eder. Ayrıca BCR Üyesi, düzeltici önlemler uygulandıktan ve durum düzeltildikten sonra İlgili Kişiyi bilgilendirecektir.

Her durumda BCR Üyeleri, İlgili Kişilerin bir AEA Denetim Kurumu nezdinde dava açma ve/veya yargısal çözüm arama hakkına sahip olmaya devam ettiğini kabul eder. BCR Üyeleri ayrıca bu hakların İlgili Kişilerin şikayet yönetimi sürecini daha önce kullanmış olmalarına bağlı olmadığını kabul eder ancak İlgili Kişiler bunu yapmaya yeniden teşvik edilir.

1. Veri koruma yönetimi

Concentrix, Ek 3’te daha ayrıntılı olarak tanımlanan bir Veri koruma organizasyonu ve yönetimi tanımlamıştır.

BCR Üyeleri, gerektiğinde ve GDPR Madde 37 uyarınca bir Veri Koruma Görevlisi veya BCR-C’ye uyumu izlemekten sorumlu olan ve bu görevin yerine getirilmesinde en yüksek yönetim desteğini alan (baş gizlilik sorumlusu gibi) başka bir kişi veya kuruluş atamayı taahhüt eder. Bu organizasyon, gizlilik iletişim noktalarından (yani Bölgesel Gizlilik Liderleri, Yerel Gizlilik Liderleri ve İş Gizlilik Danışmanlarından) oluşan bir ağa dayanan ve ilgili BCR Üyesi tarafından DPO olarak atanabilecek olan Grup Veri Koruma Görevlisi tarafından yönetilir.

Bir Denetim Kurumu tarafından resmi olarak atanan DPO, doğrudan en üst yönetim seviyesine rapor verecektir. Ayrıca DPO, görevlerini yerine getirirken herhangi bir soru veya sorun ortaya çıkarsa en üst yönetim seviyesini bilgilendirebilir.

DPO’nun çıkar çatışmasına yol açabilecek hiçbir görevi olmamalıdır. DPO ne veri koruma etki değerlendirmelerini yürütmekten ne de söz konusu durumlar bir çıkar çatışmasına yol açabilecekse BCR denetimlerini yürütmekten sorumlu olmalıdır. Bununla birlikte DPO, BCR Üyelerine yardımcı olmakta çok önemli ve yararlı bir rol oynayabilir ve bu tür görevler için DPO tavsiyesi alınmalıdır.

Mevcut ağın görev ve sorumlulukları ile çalışma yönetimi, **Ek 3 - Veri Koruma organizasyonu ve yönetimi** kapsamında daha ayrıntılı olarak tanımlanmıştır.

Ayrıca DPO, görevlerini yerine getirirken herhangi bir soru veya sorun ortaya çıkarsa en üst yönetim seviyesini bilgilendirebilir.

DPO’ya ve Bölgesel ve/veya Yerel Gizlilik Liderlerine, BCR-C Madde 7.5’te açıklanan iletişim bilgilerinden ve BCR Ek 01’de verilen yerel gizlilik irtibat kişilerinden ulaşılabilir.

1. Eğitim ve farkındalık

Kişisel Verilerin Korunması yalnızca gizlilik yasalarına uyum meselesi değil, aynı zamanda Concentrix temel değerlerinin somutlaşmış halidir. Bu bağlamda tüm çalışanları, stajyerleri ve çalışma performansındaki davranışları BCR Üyelerinin doğrudan kontrolü altında olan diğer kişileri operasyonları kapsamında İşlenen Kişisel Verilerin korunmasından sorumlu tutmak için Grup içinde bir gizlilik kültürü oluşturulması esastır.

Bu nedenle işbu BCR-C tüm kuruluş içinde uygun şekilde uygulanacaktır. Bu amaçla BCR Üyeleri; tüm Concentrix çalışanlarının, stajyerlerinin ve çalışma performansındaki davranışları BCR Üyelerinin doğrudan kontrolü altında olan diğer kişilerin işbu BCR-C’de belirtilen yükümlülük, ilke ve prosedürler hakkında gerçekten bilgi sahibi olmasını sağlamayı amaçlayan bir gizlilik eğitim programı benimsemiştir. Temel GDPR ilke ve yükümlülüklerine ek olarak, eğitim ve farkındalık programı diğerlerinin yanı sıra kamu kurumları tarafından kişisel verilere erişim taleplerinin yönetilmesine yönelik prosedürleri kapsayacaktır.

Bu eğitim; (i) Kişisel Verilere kalıcı veya düzenli erişimi olan kişilere, (ii) Kişisel Verilerin toplanmasında yer alan kişilere ve/veya (iii) Kişisel Verileri işlemek için kullanılan araçların geliştirilmesinde yer alan kişilere yöneliktir.

Eğitim materyali güncel olacak ve BCR-C'nin en son versiyonunu yansıttığından emin olmak için en azından yılda bir kez veya geçerli Veri Koruma Mevzuatında önemli değişiklikler olduğunda düzenli olarak gözden geçirilecektir.

Eğitim programının amacı şunları sağlamak olacaktır:

* Kişisel Verilerin İşlenmesinde geçerli ilkeler hakkında temel düzeyde bilgi ve mevcut prosedürler ve bunların uygulanması hakkında iyi bir anlayış,
* Kuruluş bünyesindeki farklı fonksiyonlara uyarlanmış özel eğitim.

Bu bağlamda BCR Üyelerinin BCR-C kapsamında başka bir BCR Üyesine, BCR-C'ye etkin bir şekilde tabi olmadıkça ve çalışanlarına etkili bir şekilde BCR-C hakkında uygun bir eğitim sağlamadıkça hiçbir veri aktarımı yapılamayacağını kabul ettikleri hatırlatılır.

BCR Üyeleri tüm Concentrix çalışanları, stajyerleri ve çalışma performansındaki davranışları BCR Üyelerinin doğrudan kontrolü altında olan diğer kişilerin işe ilk girdiklerinde bu eğitimi ve ardından da her yıl tazeleme eğitimi almasını sağlamayı taahhüt eder.

Bu Madde ile ilgili daha fazla ayrıntı aşağıdaki ekte verilmiştir:

* **Ek 04 – Gizlilik farkındalığı ve eğitim programı**

1. Kasten gizlilik/varsayılan gizlilik

İşbu BCR-C kapsamında tanımlanan ilkelerin etkili bir şekilde dikkate alınmasını ve gerçekleştirdiği farklı Veri İşleme faaliyetlerinde yansıtılmasını sağlamak için Concentrix, veri korumasını dikkate alacak ve herhangi bir yeni projenin en başından itibaren uygun teknik ve organizasyonel önlemleri uygulayacaktır.

Kuruluş bünyesinde Kişisel Verilere yüksek düzeyde koruma sağlamak için burada tanımlanan ilkeler ve yükümlülükler, Concentrix tarafından benimsenen kasten gizlilik prosedürleri temelinde her projenin tasarımına entegre edilecektir.

1. Şeffaflık ve işbirliği
   1. BCR-C İletişimi

BCR Üyesi, tüm İlgili Kişilere Kişisel Verilerinin işlenmesiyle ilgili olarak üçüncü taraf lehtar hakları ve bu hakları kullanma yolları hakkında bilgi sağlanacağını taahhüt eder. Söz konusu bilgiler, BCR-C Madde 7’de açıklanmıştır.

Concentrix, işbu BCR-C’yi İlgili Kişilere açık bir şekilde iletecek ve her bireyin buna kolayca erişebilmesini sağlayacaktır. Bu iletişim, İlgili Kişilerin BCR-C’nin bir kopyasını gecikmeksizin ve açık doküman formatında almasını sağlayacaktır. Buna ek olarak, işbu BCR-C'nin en son sürümünün kamuya açık bir versiyonu İlgili Kişilere her zaman Concentrix web sitesi [www.concentrix.com](http://www.concentrix.com) adresinden sunulacaktır. İlgili Kişiler ayrıca [dpo@concentrix.com](mailto:dpo@concentrix.com) adresinden DPO ile iletişime geçerek BCR-C'nin bir kopyasını talep edebilirler.

BCR-C'nin kamuya açık versiyonu en azından aşağıdaki bilgileri içerecektir:

* BCR-C kapsamına ilişkin bir açıklama (BCR-C Madde 2),
* Grubun yükümlülüğüne ilişkin madde (BCR-C Madde 7),
* Veri koruma ilkelerine ilişkin maddeler (BCR-C Madde 4, 4.1, 4.2, 4.3, 4.5, 4.6, 4.7, 4.9, 4.10 ve Madde 5),
* Veri İşlemenin yasaya uygunluğu (BCR-C Madde 4.1 ve 5),
* Güvenlik ve kişisel veri ihlali bildirimleri (BCR-C Madde 4.7 ve 4.10),
* İleriye dönük aktarımlara ilişkin kısıtlamalar (BCR-C Madde 4.9 ve Madde 6) ve
* İlgili kişilerin haklarına ilişkin maddeler (BCR-C Madde 7, 8 ve 12).

Bu bilgiler güncel olmalı ve İlgili Kişilere açık, anlaşılır ve şeffaf bir şekilde sunulmalıdır. Bu bilgiler eksiksiz olarak sağlanmalıdır, bu nedenle özetlenmesi yeterli olmayacaktır.

Kamuya açık versiyon, BCR-C'ye Ek belge olarak eklenen tüm gerekli politika ve prosedürleri de içerecektir ama özellikle BCR-C için:

* Ek 01 - A BCR-C’ye tabi olan BCR Üyeleri ve yerel gizlilik e-posta iletişim listesi
* Ek 02 Bağlayıcı Şirket Kuralları (BCR) ve Prosedür Tanımları
* Ek 05 Concentrix’in Veri Sorumlusu olarak hareket ettiği durumlarda İlgili Kişilerin taleplerine ilişkin prosedür
* Ek 11-A BCR-C maddi kapsamı: Veri İşleme Amaçları ve ilgili Kişisel Veri ve İlgili Kişiler Kategorileri Listesi

Diğer Ekler ya BCR-C için geçerli değildir ya da İlgili Kişilerin haklarını anlamaları ve/veya kullanmaları için ilgili olmayan dahili süreçlerdir.

Yukarıdaki gereklilikler, daha önce listelenen tüm bilgileri içeren BCR-C'nin basitleştirilmiş kamuya açık bir versiyonunun Concentrix web sitesinde (www.concentrix.com) bulunmasının sağlanmasıyla karşılanacaktır.

Concentrix, işbu BCR-C’yi dahili sistemler ve araçlar (ör. Concentrix Intranet, dahili iletişimler, vs.) aracılığıyla paylaşarak organizasyon bünyesinde gizlilik ve güvenlik kültürünün iyileştirilmesini teşvik edecektir.

* 1. İlgili Kişilere Sağlanan Bilgiler

BCR Üyeleri, Veri Sorumlusu olarak hareket ettiklerinde İlgili Kişilere Geçerli Veri Koruma Mevzuatı ile gerekli kılınan tüm bilgileri sağlayacaktır. BCR Üyesi, bu bilgileri gecikmeden ve Kişisel Verileri aldıktan sonra makul bir süre içinde ancak en geç bir ay içinde, yasal bir alıcıyla ilk iletişim veya ilk açıklama anında sağlayacaktır. Söz konusu bilgiler en azından aşağıdaki unsurlardan oluşacaktır:

* Veri Sorumlusunun kimlik bilgileri ve irtibat bilgileri,
* Veri Koruma Görevlisinin (DPO) ve/veya Yerel Gizlilik Liderinin iletişim bilgileri,
* Veri İşleme amaçları ve yasal dayanağı,
* Bilgiler doğrudan İlgili Kişiden toplanmadıysa İşlenen Kişisel Veri kategorileri,
* Kişisel Verilerin alıcıları,
* Uygulanabilir olduğu durumlarda, AEA dışındaki Veri Aktarımlarının varlığı, Kişisel Verilerin aktarıldığı ülkeler, yeterli düzeyde koruma sağlamak için uygulanan önlemler ve bunların bir kopyasını elde etme yolları veya bunların nerede sunulduğu,
* Veri saklama süresi,
* Yukarıda Madde 7 kapsamında tanımlandığı üzere İlgili Kişilerin hakları (ör. Veri Sorumlusundan Kişisel Verilere erişim ve Kişisel Verileri düzeltme veya silme ya da İlgili Kişiye ilişkin Veri İşlemenin kısıtlanması talebinde bulunma veya İşlemeye itiraz etme hakkı ile veri taşınabilirliği hakkının varlığı),
* Bir denetim kurumuna şikâyette bulunma hakkı,
* Kişisel Veriler İlgili Kişiden toplandığında, İlgili Kişinin (1) herhangi bir yasal veya akdi gereklilik nedeniyle Kişisel Verileri sağlamakla yükümlü olup olmadığı veya (2) bir sözleşme yapmak için gerekli olduğu için Kişisel Verileri sağlama zorunluluğu olup olmadığı ve bu tür verileri sağlamamanın olası sonuçları,
* Veri İşleme, İlgili Kişilerin onayına dayanıyorsa onayın geri çekilmesinden önce onaya dayalı Veri İşlemenin yasallığını etkilemeden onaylarını istedikleri zaman geri çekme hakkı,
* Veri İşleme, BCR Üyesinin meşru menfaatine dayanıyorsa söz konusu meşru menfaatle ilgili açıklamalar,
* Duruma göre, profilleme dahil olmak üzere otomatik karar almanın varlığı ve
* Kişisel Veriler, İlgili Kişiden toplanmadığında bunların kaynağına ilişkin mevcut bilgiler (ör. özellikle Kişisel Veri kategorileri, Kişisel Verilerin ilk kaynağı, Kişisel Verilerin kamusal niteliği).

BCR Üyeleri, bu bilgileri İlgili Kişilere erişilebilir, kolay anlaşılır, net, açık ve sade bir dille sağlamayı taahhüt eder.

* 1. BCR-C'ye uyumu etkileyen yerel mevzuat ve uygulamalarla tutarsızlıklar

BCR Üyeleri, BCR-C'yi yalnızca Veri Alıcısı olarak hareket eden BCR Üyesi tarafından Kişisel Verilerin İşlenmesine uygulanabilir olan Yetersiz üçüncü bir hedef ülkedeki yasa ve uygulamaların, Kişisel Verileri ifşa etme gereklilikleri veya kamu otoriteleri tarafından erişime izin veren önlemler dahil olmak üzere, bu BCR-C kapsamındaki yükümlülüklerini yerine getirmesini engellemediğini değerlendirdikleri durumlarda Veri Aktarımları için bir araç olarak kullanmayı taahhüt ederler.

Söz konusu taahhüt, temel hak ve özgürlüklerin özüne saygı gösteren ve aşağıda listelenen amaçlardan birini korumak için demokratik bir toplumda gerekli ve orantılı olanı aşmayan yasa ve uygulamaların BCR-C ile çelişmediği anlayışına dayanmaktadır:

1. Ulusal güvenlik ve/veya
2. Savunma ve/veya
3. Kamu güvenliği ve/veya
4. Suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması veya kamu güvenliğine yönelik tehditlerin önlenmesi ve bunlara karşı koruma sağlanması da dahil olmak üzere cezai yaptırımların uygulanması ve/veya
5. Birliğin veya bir Üye Devletin genel kamu menfaatinin diğer önemli hedefleri, özellikle Birliğin veya bir Üye Devletin parasal, bütçesel ve vergi konuları, kamu sağlığı ve sosyal güvenlik de dahil olmak üzere önemli bir ekonomik veya mali menfaati ve/veya
6. Yargı bağımsızlığının ve adli muamelelerin korunması ve/veya
7. Düzenlemeye tabi meslekler için etik kural ihlallerinin önlenmesi, soruşturulması, tespiti ve kovuşturulması ve/veya
8. (a) ila (e) ve (g) noktalarında belirtilen durumlarda, ara sıra bile olsa, resmi otoritenin uygulanmasıyla bağlantılı bir izleme, teftiş veya düzenleyici işlev ve/veya
9. İlgili Kişinin veya başkalarının hak ve özgürlüklerinin korunması ve/veya
10. kamu davalarının yürütülmesi.

BCR-C'de yer alan taahhütlere saygı duyulmasını etkileyebilecek Yetersiz Üçüncü bir Ülkenin yasa ve uygulamalarının değerlendirilmesinde, BCR Üyeleri özellikle aşağıdaki unsurları dikkate alacaktır:

* **Veri Aktarımları veya Aktarım setinin özel koşulları** ve aşağıdakiler dahil olmak üzere aynı üçüncü ülke içinde veya başka bir Yetersiz Üçüncü ülkeye öngörülen ileriye dönük Veri Aktarımlarının özel koşulları:
* Kişisel Verilerin aktarılma ve işlenme amaçları (ör. pazarlama, İK, depolama, BT desteği, klinik deneyler),
* Veri İşleme sürecine dahil olan kuruluş türleri (Veri Alıcısı ve herhangi bir ileriye dönük Aktarımın daha sonraki alıcısı),
* Veri Aktarımı veya Aktarım setinin gerçekleştiği ekonomik sektör,
* Aktarılan Kişisel Verilerin kategorileri ve biçimi,
* Depolama dahil olmak üzere Veri İşlemenin yeri ve
* Kullanılan iletim kanalları.
* **Hedef üçüncü ülkenin yasa ve uygulamaları**; verilerin kamu kurumlarına açıklanmasını veya bu kurumlar tarafından erişime izin verilmesini gerektirenler ve Veri Sağlayıcısı ülke ile Veri Alıcısı ülke arasındaki aktarım sırasında bu Kişisel Verilere erişim sağlayanlar da dahil olmak üzere aktarımın koşulları ışığında ilgili olan hedef üçüncü ülke yasa ve uygulamaları ile geçerli sınırlamalar ve güvenlik önlemleri.
* **İlgili akdi, teknik veya organizasyonel güvenlik önlemleri**; hem veri aktarımı sırasında uygulanan hem de hedef ülkede Kişisel Verilerin İşlenmesine uygulanan önlemler dahil BCR-C kapsamındaki güvenlik önlemlerini tamamlamak için uygulananlar.

BCR-C kapsamında öngörülenlere ek olarak herhangi bir güvenlik önlemi uygulanması gerektiğinde Sorumlu BCR Üyesi olarak Webhelp SAS, DPO ve ilgili Yerel Gizlilik Lideri bilgilendirilecek ve bu değerlendirmeye dahil edilecektir.

BCR Üyeleri, bu değerlendirmenin yanı sıra seçilen ve uygulanan ek önlemleri uygun şekilde belgelendirecektir. Bu belgeler, talep edilmesi halinde yetkili Denetim Kurumuna ve DPO’ya sunulacaktır.

Ayrıca Veri Alıcısı olarak hareket eden BCR Üyesi, işbu BCR-C'yi Veri Aktarımları için bir araç olarak kullanırken ve BCR üyeliği süresince, Yetersiz Üçüncü Ülke yasalarında bir değişiklik veya bir önlem (örneğin bir ifşa talebi) sonrasında dahil olmak üzere BCR-C kapsamındaki yükümlülüklerini yerine getirmesini engelleyecek yasa veya uygulamalara tabi olduğuna veya tabi hale geldiğine inanmak için nedenleri varsa Veri Sağlayıcısını derhal bilgilendirecektir. Bu bilgiler ayrıca Sorumlu BCR Üyesine ve DPO'ya da sağlanmalıdır.

Bu bildirimin doğrulanması üzerine Sorumlu BCR Üyesinin yanı sıra Veri Sağlayıcısı olarak hareket eden BCR Üyesi; DPO, ilgili Yerel Gizlilik Lideri ve Bilgi Güvenliği ekibinin yardımıyla BCR-C kapsamındaki yükümlülüklerin yerine getirilmesini sağlamak için Veri Sağlayıcısı ve/veya Veri Alıcısı olarak hareket eden BCR Üyesi tarafından benimsenecek olan ek önlemleri (ör. güvenliği ve gizliliği sağlamak için teknik veya organizasyonel önlemler) derhal belirlemeyi taahhüt etmelidir. Aynı durum Veri Sağlayıcısı olarak hareket eden bir BCR Üyesinin, Veri Alıcısı olarak hareket eden bir BCR Üyesinin artık işbu BCR-C kapsamındaki yükümlülüklerini yerine getiremeyeceğine inanmak için nedenleri olması durumunda da geçerlidir.

Veri Sağlayıcısı olarak hareket eden BCR Üyesi (Sorumlu BCR Üyesi ve DPO ve/veya ilgili Yerel Gizlilik Lideri ile birlikte), bir Veri Aktarımı veya bir dizi Veri Aktarımı için ek önlemlerle birlikte olsa bile BCR-C’ye uyulamayacağını değerlendirirse ya da yetkili Denetim Kurumu tarafından talimat verilirse BCR Üyesi, söz konusu Veri Aktarımını veya bir dizi Veri Aktarımı ile aynı değerlendirme ve gerekçelendirmenin benzer bir sonuca yol açacağı tüm Veri Aktarımlarını uyum tekrar sağlanana veya Veri Aktarımı sonlandırılana kadar askıya almayı taahhüt eder.

Böyle bir askıya almanın ardından Veri Sağlayıcısı olarak hareket eden BCR Üyesi, BCR-C'ye uyulamaması ve BCR'ye uyumun askıya alınmasından itibaren bir ay içinde düzeltilememesi halinde Veri Aktarımını veya bir dizi Veri Aktarımını sonlandırmak zorundadır. Bu durumda, askıya almadan önce aktarılmış olan Kişisel Veriler ve bunların kopyaları, Veri Sağlayıcısı olarak hareket eden BCR Üyesinin tercihi üzerine kendisine iade edilmeli veya tamamen imha edilmelidir.

Sorumlu BCR Üyesi olarak Webhelp SAS ve DPO ve/veya ilgili yerel Gizlilik Lideri, tüm diğer BCR Üyelerini yapılan değerlendirme ve bunun sonuçları hakkında bilgilendirecek, böylece aynı türde Aktarımlar başka bir BCR Üyesi tarafından gerçekleştirilirse belirlenen ek önlemler uygulanacaktır ya da etkili ek önlemler alınamazsa mevcut Veri Aktarımları askıya alınır veya sonlandırılır.

Veri Sağlayıcıları olarak hareket eden BCR Üyesi, sürekli olarak ve uygun durumlarda Veri Alıcıları ile işbirliği içinde Veri Sağlayıcıların koruma düzeyinin ilk değerlendirmesini ve buna göre bu Aktarımlar hakkında alınan kararları etkileyebilecek Kişisel Verileri aktarmış olduğu Yetersiz Üçüncü Ülkelerdeki gelişmeleri izleyecektir.

* 1. İşbirliği yapma görevi

Her durumda BCR Üyeleri, Denetim Kurumları tarafından denetlenmeyi veya (yerinde veya uzaktan) teftiş edilmeyi kabul etmek suretiyle dahil olmak üzere AEA Denetim Kurumlarıyla işbirliği yapmayı, tavsiyeleri dikkate almayı ve işbu BCR-C ile ilgili olarak sağlanabilecek yetkili EEA Denetim Kurumunun kararına tabi olmayı kabul eder. BCR Üyeleri, yetkili Denetim Kurumunun yetkileri ve denetim haklarının, özellikle söz konusu Denetim Kurumu tarafından yürütülen pratik denetimle ilgili olarak sınırlandırılamayacağını kabul eder ve onaylar.

BCR Üyeleri ve uygun olduğunda ilgili temsilcileri, talep edilmesi halinde BCR-C kapsamındaki veri işleme faaliyetlerine ilişkin kayıtlar gibi bilgileri AEA Denetim Kurumuna sunacaktır.

Yetkili Denetim Kurumunun BCR-C'ye uyumun denetimini yapmasıyla ilgili herhangi bir anlaşmazlık söz konusu Denetim Kurumunun Üye Devletinin mahkemeleri tarafından, bu Üye Devletin usul hukukuna uygun olarak çözülecektir. BCR Üyeleri kendilerini bu mahkemelerin yargı yetkisine tabi tutmayı kabul ederler.

1. BCR’yi kapsayan denetim programı

Veri Sorumlusu olarak hareket eden her BCR Üyesi, BCR-C'ye uyumdan sorumlu olacak ve bu uyumu gösterebilecektir. Bu amaçla ve Madde 4.4 (Kayıt Tutma), 4.8 (Veri Koruma Etki Değerlendirmesi) ve Ek 08 - Kişisel Veri İhlali Bildirimi’nde belirtilen gerekliliklere ek olarak BCR Üyeleri veri koruma denetim programıyla ilgili aşağıdaki gerekliliğe uyacaktır.

BCR Üyesi, denetim programını geliştirmeyi ve işbu BCR-C’ye uyumunun incelenmesini denetim programına entegre etmeyi taahhüt eder. Denetim programı, şunları tanımlamayı sağlayacaktır:

* Denetimlerin gerçekleştirileceği makul bir sıklık,
* Denetimin beklenen kapsamı ve
* Denetimden sorumlu ekip.

Denetim prosedürü, **Ek 7 – Veri Gizliliği Denetimleri Prosedürleri**’nde ayrıntılı olarak açıklanmıştır. Denetim, düzeltici aksiyonların alınmasını sağlayacak yöntemler ve aksiyon planları dahil olmak üzere işbu BCR-C’nin tüm yönlerini (örneğin; uygulamalar, BT sistemleri, kişisel verileri işleyen veri tabanları veya ileriye dönük aktarımlar, BCR-C ile çelişen ulusal yasalar kapsamındaki zorunlu gerekliliklerle ilgili alınan kararlar, Gruptan veri sorumlularına veya veri işleyenlere yapılan aktarımlar için kullanılan sözleşme şartlarının incelenmesi, düzeltici aksiyonlar, vs.) kapsar. Bununla birlikte bir BCR Üyesi için BCR-C’nin tüm yönleri uygun düzenli aralıklarla izlendiği sürece, söz konusu BCR Üyesi her denetlendiğinde bu tür bir denetim programının BCR-C’nin tüm yönlerini izlemesi gerekmez.

BCR Üyeleri, BCR-C'ye uyumun doğrulanmasını veya işbu BCR-C kapsamına giren bir Veri İşleme faaliyetinin İlgili Kişilerin hak ve özgürlükleri üzerindeki risk seviyesinin dikkate alınmasını sağlamak için düzenli olarak (en azından yılda bir kez ve/veya uyumsuzluk belirtileri varsa) denetimler yapılmasını taahhüt eder.

Düzenli denetimlere ek olarak, DPO ve/veya ilgili gizlilik ağı üyesi (ör. Yerel Gizlilik Lideri) ya da Concentrix Grubu’ndaki iç denetim departmanı gibi diğer bir yetkili fonksiyon tarafından özel denetimler (ad hoc denetimler) talep edilebilir. Söz konusu denetimler, DPO ve/veya ilgili gizlilik ağı üyesi tarafından tavsiye edilen dahili ve/veya harici akredite denetçiler tarafından gerçekleştirilebilir. Yol haritası, Ek 7’de belirtildiği gibi DPO ve/veya ilgili gizlilik ağı üyesi tarafından başlatılır ve belirlenir. Her halükarda harici denetçiler bağımsız, bir gizlilik yükümlülüğüne tabi ve/veya uygun bir yasal gizlilik yükümlülüğü altında olacaktır.

DPO, gerçekleştirilecek denetimlerin kapsamını belirlemekten sorumludur. Bu amaçla Gizlilik Komitesine danışabilir ve/veya söz konusu denetimin kapsamını belirlemek üzere Concentrix’in iç denetim ekibine güvenebilir. Denetim, aşağıdaki koşullar sağlandığı takdirde Grup DPO’su ve/veya ilgili gizlilik ağı üyeleri (ör. Yerel Gizlilik Lideri) ve/veya Concentrix Grubu’nun iç denetim ekibi veya Concentrix bünyesindeki başka bir ilgili fonksiyon tarafından yapılabilir:

* Sorumlu kişilere, bu denetimlere ilişkin görevlerinin yerine getirilmesi konusunda bağımsızlık güvencesi verilmesi ve
* BCR-C'ye uyumu denetlemekten sorumlu kişiler için söz konusu durumun bir çıkar çatışmasına yol açması.

Her denetimin sonucu, bilgi amaçlı Grup DPO’suna ve/veya ilgili gizlilik ağı üyelerine (ör. Yerel Gizlilik Liderleri) ve/veya Gizlilik Komitesi ve/veya Webhelp SAS yönetim kurulu üyelerine sunulacaktır. Nihai rapor, kusur tespiti ve düzeltici aksiyonlar Yerel Gizlilik Lideri tarafından paylaşılacak ve uygulanacaktır. Yerel Gizlilik Lideri değerlendirmesine dayanarak rapor, uygun olduğu hallerde herhangi bir İş Gizlilik Uzmanı, yerel güvenlik yöneticisi, süreç/sistem sorumluları, Concenrix Grubu nihai ana şirketinin yönetim kurulu veya denetime tabi ilgili BCR Üyesinin yönetim kurulu veya herhangi bir diğer gerekli kurum içi çalışanla da paylaşılabilir. Öncelikli olarak söz konusu önlemlerin uygulanmasıyla birlikte düzeltici aksiyonlar tanımlanacaktır.

Concentrix, yetkili AEA Denetim Kurumlarının denetim sonuçlarının iletilmesini talep edebileceklerini ve dolayısıyla talep edilmesi halinden bunlara erişim imkanı tanımayı kabul ettiklerini onaylar. Denetim raporlarının ve ilgili iç denetim raporlarının sonuçları, AEA’da bulunan Denetim Kurumlarının aşağıda belirtilen denetim haklarını kullanmaları halinde bunlara erişebilecekleri bir biçimde tutulacaktır.

BCR Üyeleri, Yetkili Denetim Kurumlarının talep etmeleri halinde denetim sonuçlarına erişebilmesini sağlamayı taahhüt eder ve özellikle ticari sırların korunması gibi bir gizlilik gerekçesiyle bu hakları sınırlamaz.

BCR Üyesinin herhangi bir yetkili AEA Denetim Kurumuna BCR-C ile ilgili herhangi bir konuda veri koruma denetimleri yapma yetkisi vereceği hatırlatılır. Bu bağlamda her BCR Üyesi, AEA Denetim Kurumunun BCR Üyelerinin işbu BCR-C'ye uyumunu göstermek için gerekli bilgileri elde edebilmesi için ilgili BCR Üyesini denetlemesine izin verecektir (ayrıca bkz. yukarıda Madde 12.4).

1. BCR-C’de değişiklik

Concentrix DPO, Yerel Gizlilik Liderlerinin desteğiyle işbu BCR-C’nin güncel tutulmasını sağlayacaktır (örneğin; düzenleyici ortamda yapılan değişiklikleri, AB veri koruma kurumlarının önerilerini veya BCR-C kapsamındaki değişiklikleri hesaba katmak için).

Özellikle DPO, BCR-C’ye tabi olan kuruluşların listesini güncel tutacaktır. Concentrix’in herhangi bir yeni kuruluşu BCR-C’ye etkin bir şekilde tabi olduğunda (Madde 3.2’de belirtildiği üzere) DPO bu listeyi güncelleyecek ve fazla gecikmeden tüm BCR Üyelerini ve ilgili AEA Denetim Kurumlarını yetkili AEA Denetim Kurumu vasıtasıyla bilgilendirecektir. Bu tür güncellenmiş bilgiler, İlgili Kişilere BCR-C ile birlikte ve aynı yollarla sunulacaktır.

Webhelp SAS, bu tür değişiklikleri yılda en az bir kez veya DPO tarafından gerekli görüldüğünde yetkili AEA Denetim Kurumlarına bildirecektir. Söz konusu değişiklikler, AEA Denetim Kurumlarına yılda en az bir kez güncellemeyi gerekçelendiren nedenlerin kısa bir açıklamasıyla birlikte yetkili AEA Denetim Kurumu vasıtasıyla bildirilecektir. Hiçbir değişiklik yapılmadığında da Denetim Kurumlarına aynı süreci takiben yılda bir kez bildirim yapılmalıdır.

Yıllık güncelleme veya bildirim, Sorumlu BCR Üyesi olarak Webhelp SAS'ın, BCR-C'nin AEA dışındaki BCR Üyeleri tarafından ihlalinden kaynaklı zararların tazminini sağlamak için uygun düzenlemeler yaptığına ilişkin teyidin yenilenmesini de içermelidir.

Bir değişikliğin BCR-C üzerinde veya işbu BCR-C tarafından verilen hakların korunma seviyesi üzerinde önemli bir etkisi olduğu ölçüde Webhelp SAS, DPO'nun yardımıyla BCR Üyelerini ve AEA Denetim Kurumlarını derhal bilgilendirmeyi taahhüt eder.

1. BCR-C'ye uyulmaması

Veri Sağlayıcısı ve Veri Alıcısı, bir BCR Üyesi olarak aşağıdaki gerekliliklere uyacaktır:

* Bir BCR üyesi BCR-C’ye etkin bir şekilde tabi olmadığı ve buna uyumu sağlayamadığı sürece bu BCR üyesine hiçbir veri aktarımı yapılmaz.
* Veri Alıcısı, yukarıda BCR-C Madde 12.3’de daha ayrıntılı olarak açıklanan durumlar dahil olmak üzere herhangi bir nedenle BCR-C'ye uyamadığı takdirde Veri Sağlayıcısını derhal bilgilendirmelidir.
* Veri Alıcısı, BCR-C’yi ihlal eder veya BCR-C’ye uyamazsa Veri Sağlayıcısı Veri Aktarımını askıya almalıdır (bkz. yukarıda BCR-C Madde 12.3).

Veri Alıcısı, aşağıdaki durumlarda Veri Sağlayıcısının tercihi üzerine BCR-C kapsamında Aktarılmış olan Kişisel Verileri derhal iade edecek veya silecektir:

* Veri Sağlayıcısı veri aktarımını askıya almışsa ve işbu BCR-C’ye uyum makul bir süre içinde ve her halükarda askıya alınmadan itibaren bir ay içinde düzeltilmezse,
* Veri Alıcısı, BCR-C'yi önemli veya sürekli olarak ihlal ediyorsa,
* Veri Alıcısı, BCR-C kapsamındaki yükümlülüklerine ilişkin yetkili bir mahkemenin veya Yetkili Denetim Kurumunun bağlayıcı bir kararına uymuyorsa.

Aynı taahhütler, verilerin tüm kopyaları için geçerli olmalıdır. Veri Alıcısı, verilerin silindiğini Veri Sağlayıcısına onaylamalıdır.

Veriler silinene veya iade edilene kadar Veri Alıcısı, BCR-C'ye uyumu sağlamaya devam etmelidir.

Veri Alıcısı için geçerli yerel yasaların aktarılmış olan Kişisel Verilerin iadesini veya silinmesini yasaklaması durumunda Veri Alıcısı, BCR-C'ye uyumu sağlamaya devam edeceğini ve verileri yalnızca bu yerel yasa uyarınca gerekli olduğu ölçüde ve süre boyunca işleyeceğini garanti etmelidir.

Yürürlükteki yerel yasaların ve/veya uygulamaların BCR-C'ye uyumu etkilediği durumlar için, bkz. yukarıda BCR-C Madde 12.3.

1. Fesih

Veri alıcısı olarak hareket eden ve BCR-C'ye tabi olmaktan çıkan bir BCR Üyesi, BCR-C kapsamında alınan Kişisel Verileri saklayabilir, iade edebilir veya silebilir.

Veri Sağlayıcısı ve Veri Alıcısı, verilerin Veri Alıcısı tarafından saklanabileceği hususunda anlaşırsa GDPR Bölüm V doğrultusunda ve BCR-C Madde 6’da yansıtıldığı şekilde koruma sürdürülmelidir.

1. Ekler

* Ek 01 - BCR-P’ye tabi Concentrix kuruluşları ve yerel gizlilik e-posta iletişim listesi
* Ek 02 - Bağlayıcı Şirket Kuralları (BCR) ve Prosedür Tanımları
* Ek 03 - Gizlilik yönetimi ve organizasyonu
* Ek 04 - Gizlilik farkındalığı ve eğitim programı
* Ek 05 BCR Üyelerinin Veri Sorumlusu olarak hareket ettiği durumlarda İlgili Kişilerin taleplerine ilişkin prosedür
* Ek 06 - BCR Üyelerinin Veri İşleyen olarak hareket ettiği durumlarda İlgili Kişilerin taleplerine ilişkin prosedür
* Ek 07 - Denetim Prosedürü
* Ek 08 - Kişisel Verilerin İhlali Prosedürü
* Ek 09 - Veri Koruma Etki Değerlendirmesi
* Ek 10 - Bilgi Güvenlik Politikası
* Ek 11-A Veri İşleme Amaçları ve ilgili Kişisel Veri ve İlgili Kişi Kategorileri BCR-C Listesi (Maddi Kapsam)
* Ek 11-B Veri İşleme Amaçları ve ilgili Kişisel Veri ve İlgili Kişi Kategorileri BCR-P Listesi (Maddi Kapsam)

BELGE KONTROLÜ

|  |  |  |
| --- | --- | --- |
| Versiyon | Güncelleme | Değişiklik Özeti |
| 0.1 | 27/02/2022 | Son Onay |
| 0.2 | 01/01/2023 | BCR Üyeleri listesinin güncellenmesi |
| 0.3 | 24/02/2023 | BCR Üyeleri listesinin güncellenmesi |
| 0.4 | 01/04/2024 | Yeniden markalama ve biçimlendirme  WP256\_Rev01’i yürürlükten kaldırarak yerini alan EDPB Tavsiyeleri 1/2022 ile uyum |

|  |  |
| --- | --- |
| İnceleme Sıklığı | Bu belge en az yılda bir kez veya Webhelp kuruluşlarında değişiklik olduğunda gözden geçirilecektir. |
| Düzenleme Tarihi | 25/05/2018 |
| Alan | Gizlilik |
| Sınıflandırma | Kamuya Açık |
| Referans | EN\_\_GPPriv-01- Bağlayıcı Şirket Kuralları - Veri Sorumlusu |