BAHÇEŞEHİR ÜNİVERSİTESİ

KİŞİSEL VERİLERİN KORUNMASI VE VERİ MAHREMİYETİ POLİTİKASI

1. Amaç

Bahçeşehir Üniversitesi, kişisel verilerin korunmasını bireylerin temel hak ve özgürlüklerinin, özel hayatın gizliliğinin, kurumsal güvenin ve sorumlu veri yönetiminin ayrılmaz bir unsuru olarak kabul eder.

Bu politikanın amacı; Bahçeşehir Üniversitesi bünyesinde gerçekleştirilen kişisel veri işleme faaliyetlerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili ikincil düzenlemelere uygun biçimde yürütülmesine ilişkin kurumsal yaklaşımı, temel ilkeleri, görev ve sorumlulukları belirlemektir.

Bahçeşehir Üniversitesi, kişisel verilerin eğitim-öğretim, araştırma, toplumsal katkı, idari, akademik, operasyonel ve yönetsel süreçlerde hukuka uygun, güvenli, şeffaf, hesap verebilir ve işlendikleri amaçla bağlantılı, sınırlı ve ölçülü biçimde kullanılmasını esas alır.

Bu politika, Üniversitenin kişisel verilerin korunmasına ilişkin üst düzey kurumsal çerçevesini oluşturur. Uygulamaya ilişkin operasyonel, hukuki ve teknik ayrıntılar Üniversitenin ilgili politika, prosedür, yönerge, usul ve esasları, rehberleri, sözleşmeleri ve diğer kurumsal düzenlemeleriyle belirlenir.

2. Kapsam

2.1. Bu politika, Bahçeşehir Üniversitesi tüzel kişiliği tarafından veri sorumlusu veya veri işleyen sıfatıyla gerçekleştirilen kişisel veri işleme faaliyetlerini kapsar.

Politika;

a) Tam ve yarı zamanlı akademik personeli,

b) İdari personeli,

c) Öğrencileri ve mezunları,

ç) Aday öğrencileri,

d) Araştırmacıları ve proje personelini,

e) Misafir akademisyenleri ve araştırmacıları,

f) Stajyerleri ve bursiyerleri,

g) Danışmanları,

ğ) Üniversite adına hizmet sunan hizmet sağlayıcı ve taşeron personelini,

h) Komite, kurul ve jüri çalışmalarına dışarıdan katılan kişileri,

ı) Kampüs ziyaretçilerini,

i) Üniversite adına veya Üniversiteye ait verileri kullanarak faaliyet yürüten diğer gerçek ve tüzel kişileri

kapsar.

2.2.Öğrencilerin eğitim, araştırma, proje, staj, uygulama, toplumsal katkı veya diğer faaliyetlerde Bahçeşehir Üniversitesine ait ya da Üniversite tarafından işlenen kişisel verilere eriştiği veya bu verileri kullandığı durumlar bu politika kapsamındadır.

2.3.Kişilerin, KVKK'nın 28. maddesinin 1. fıkrasının (a) bendi uyarınca tamamen kendileriyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetleri çerçevesinde gerçekleştirdikleri kişisel veri işleme faaliyetleri bu politikanın kapsamı dışındadır. Ancak ilgili kişilerin, Üniversitenin veri sorumluluğunda bulunan veya Üniversite süreçleri kapsamında erişim sağladıkları kişisel verileri kurumsal amaç ve yetkileri dışında işlemeleri, bu politikanın ve ilgili kurumsal düzenlemelerin ihlali niteliğindedir.

2.4.Ayrı tüzel kişiliğe sahip kuruluşlar bu politikanın doğrudan kapsamında değildir. Bu kuruluşlarla yürütülen faaliyetlerde tarafların veri sorumlusu veya veri işleyen sıfatları, kişisel veri işleme faaliyetinin niteliğine göre belirlenir ve gerekli sözleşmelerle düzenlenir.

3. Temel Yaklaşım ve İlkeler

Bahçeşehir Üniversitesi, kişisel verilerin korunmasını yalnızca bilgi teknolojileri veya hukuki uyum konusu olarak değerlendirmez. Kişisel verilerin korunması, Üniversitenin akademik ve idari süreçlerinin tamamında ortak sorumluluk gerektiren kurumsal bir yönetim alanıdır. Bahçeşehir Üniversitesi, kişisel verilerin işlenmesinde aşağıdaki temel ilkeleri benimser:

3.1. Hukuka ve Dürüstlük Kurallarına Uygunluk

Kişisel veriler, Kişisel Verilerin Korunması Kanunu, ilgili ikincil düzenlemeler ve Üniversitenin kurumsal düzenlemelerine uygun biçimde işlenir. Veri işleme faaliyetlerinde ilgili kişilerin hakları ve makul beklentileri gözetilir.

3.2. Doğruluk ve Güncellik

Kişisel verilerin doğru ve gerektiğinde güncel olması esas alınır. Eksik veya yanlış olduğu tespit edilen verilerin düzeltilmesine yönelik gerekli süreçler yürütülür.

3.3. Belirli, Açık ve Meşru Amaçlar İçin İşleme

Kişisel veriler, önceden belirlenmiş, açık ve meşru amaçlar doğrultusunda işlenir. Verilerin belirlenen amaçlarla bağdaşmayan biçimde kullanılmaması esastır.

3.4. İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

Kişisel veriler, işleme amacının gerektirdiği ölçüde toplanır, kullanılır ve saklanır. Kişisel verilere erişim, görev, yetki ve kurumsal ihtiyaçlarla sınırlandırılır.

3.5. Gerekli Süre Kadar Muhafaza

Kişisel veriler, ilgili mevzuatta öngörülen veya işleme amacının gerektirdiği süre boyunca saklanır. Saklama süresi sona eren kişisel veriler, ilgili kurumsal düzenlemeler doğrultusunda silinir, yok edilir veya anonim hâle getirilir.

3.6. Şeffaflık

İlgili kişiler, kişisel verilerinin işlenme amaçları, hukuki sebepleri, toplanma yöntemleri ve aktarılabileceği alıcı grupları hakkında açık ve anlaşılır biçimde bilgilendirilir.

3.7. Hesap Verebilirlik

Üniversite, kişisel veri işleme faaliyetlerinin Kişisel Verilerin Korunması Kanunu ve ilgili kurumsal düzenlemelere uygunluğunu gösterecek kayıtları, envanterleri, sözleşmeleri ve diğer kurumsal belgeleri oluşturur ve güncel tutar.

3.8. Gizlilik, Bütünlük ve Erişilebilirlik

Kişisel verilerin yetkisiz erişim, açıklama, değiştirme, kayıp, bozulma veya imhaya karşı korunması için uygun teknik ve idari tedbirler alınır.

Bu politika bir aydınlatma metni değildir. Belirli kişisel veri işleme faaliyetlerine ilişkin aydınlatma metinleri, ilgili faaliyetin niteliği ve Kişisel Veri İşleme Envanterindeki güncel bilgiler esas alınarak ayrıca hazırlanır.

4. Kişisel Verilerin İşlenmesi ve Kişisel Veri İşleme Envanteri

4.1. Bahçeşehir Üniversitesi, kişisel verileri yalnızca Kişisel Verilerin Korunması Kanununda düzenlenen Kişisel Verilerin İşlenme Şartlarından veya hukuki sebeplerden en az birinin bulunması hâlinde işler.

4.2. Açık rıza, kişisel veri işlemenin tek veya varsayılan hukuki sebebi değildir. İşleme faaliyetinin başka bir hukuki sebebe dayanması mümkün olduğunda ilgili işleme şartı esas alınır. Açık rıza, yalnızca faaliyetin niteliği veya mevzuat gereği ihtiyaç duyulan durumlarda alınır.

4.3. Üniversitenin kişisel veri işleme faaliyetleri Kişisel Veri İşleme Envanterinde kayıt altına alınır. Envanter; aydınlatma metinlerinin, saklama ve imha süreçlerinin, veri aktarım düzenlemelerinin ve kişisel veri yönetimine ilişkin diğer kurumsal uygulamaların temel kaynağıdır.

4.4. Akademik ve idari birimler, kendi faaliyet alanlarındaki kişisel veri işleme süreçlerinin doğru ve güncel biçimde envantere yansıtılmasına katkı sağlar.

4.5. Yeni veya önemli ölçüde değişen veri işleme faaliyetleri, sistemler, yazılımlar, dijital platformlar, araştırma projeleri, yapay zekâ uygulamaları ve dış hizmet alımları devreye alınmadan önce ilgili mevzuat, bilgi güvenliği ve kurumsal sorumluluklar bakımından değerlendirilir.

5. İlgili Kişilerin Hakları

5.1. İlgili kişilerin, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuat kapsamında tanınan tüm hakları saklıdır.

5.2. İlgili kişiler, kişisel verilerinin işlenmesine ilişkin haklarını, ilgili mevzuatta öngörülen usul ve esaslar çerçevesinde Üniversiteye başvurarak kullanabilir.

5.3. Başvurular, kvkk@bau.edu.tr adresi veya Üniversite tarafından ilan edilen diğer başvuru kanalları üzerinden iletilebilir.

5.4. İlgili kişi başvurularının hukuki değerlendirmesi ve yanıtlanması Veri Sorumlusu adına Hukuk Müşavirliği koordinasyonunda yürütülür. Başvuruların teknik tespiti, sistem kayıtlarının incelenmesi ve operasyonel süreçlerin yürütülmesinde Bilgi İşlem Daire Başkanlığı ve ilgili akademik/idari birimler gerekli bilgi ve belge desteğini sağlar.

5.5. Başvurular, ilgili mevzuatta öngörülen usul ve süreler içerisinde sonuçlandırılır.

6. Üniversite Faaliyetlerinde Kişisel Verilerin Korunması

6.1. Eğitim-Öğretim Süreçleri

6.1.1. Öğrencilere ait kişisel veriler; kayıt, eğitim-öğretim, ölçme-değerlendirme, akademik danışmanlık, destek hizmetleri, staj, mezuniyet ve diğer akademik süreçlerin yürütülmesi amacıyla ve bu süreçlerin gerektirdiği ölçüde işlenir.

6.1.2. Öğrenci verileri yetkisiz kişilere açıklanamaz, kurumsal amaç dışında kullanılamaz ve Üniversite tarafından onaylanmamış sistemlere aktarılamaz.

6.1.3. Öğretim elemanları ve öğrenciler; ders, sınav, ödev, proje, tez, staj ve diğer akademik faaliyetlerde kişisel verilerin korunmasına ilişkin yükümlülüklere uyar.

6.2. Araştırma Süreçleri

6.2.1. Araştırma faaliyetlerinde kullanılan kişisel veriler; bilimsel etik, araştırma bütünlüğü, ilgili kişi hakları, veri güvenliği ve gerekli etik kurul süreçleri gözetilerek işlenir.

6.2.2. Araştırma yürütücüleri, araştırma kapsamında işlenen kişisel verilerin hukuka uygunluğu, güvenliği, erişim yetkileri, saklanması ve araştırma sona erdiğinde yapılacak işlemler bakımından sorumluluk taşır.

6.2.3. Ortak araştırma faaliyetlerinde tarafların veri sorumlusu veya veri işleyen sıfatları ile kişisel verilere ilişkin görev ve yükümlülükleri sözleşmelerle belirlenir.

6.3. İdari, Operasyonel ve Yönetsel Süreçler

6.3.1. Çalışan, öğrenci, mezun, aday öğrenci, ziyaretçi, tedarikçi ve diğer ilgili kişilere ait veriler; Üniversitenin insan kaynakları, öğrenci hizmetleri, mali işler, güvenlik, iletişim, sözleşme yönetimi, kalite güvencesi ve diğer kurumsal faaliyetlerinin yürütülmesi amacıyla işlenebilir.

6.3.2. Kişisel veriler yalnızca yetkilendirilmiş kişiler tarafından ve görevle sınırlı olarak kullanılır. Kişileri önemli ölçüde etkileyen akademik, idari ve yönetsel kararlarda nihai değerlendirme ve sorumluluğun yetkili kişilerde bulunması esastır.

6.4. Hassas Veriler ve Özel Koruma Gerektiren Faaliyetler

6.4.1. Hassas verilerin ve kişilerin temel hak ve özgürlükleri üzerinde önemli etki doğurabilecek kişisel veri işleme faaliyetlerinin yürütülmesinde daha sıkı teknik, idari ve hukuki tedbirler uygulanır.

6.4.2. Hassas verilere erişim, yalnızca görevi gereği erişmesi gereken yetkili kişilerle sınırlandırılır.

6.4.3. Kapsamlı izleme, profilleme, münhasıran otomatik sistemler vasıtasıyla analiz, büyük ölçekli veri işleme ve benzeri faaliyetler uygulanmadan önce ilgili kurumsal birimlerin değerlendirmesine tabi tutulur.

7. Veri Güvenliği, Saklama ve İmha

7.1.1. Bahçeşehir Üniversitesi, kişisel verilerin hukuka aykırı olarak işlenmesini veya kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin güvenli biçimde

muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri alır.

7.1.2. Kişisel verilerin gizliliği, bütünlüğü ve erişilebilirliği; görev ve yetkilendirme esaslı erişim, kurumsal bilgi güvenliği uygulamaları, kayıt ve izleme mekanizmaları ile korunur.

7.1.3. Teknik ve operasyonel güvenlik tedbirleri, Üniversitenin bilgi güvenliği, erişim, cihaz, ağ, veri tabanı, tedarikçi, saklama ve imha düzenlemeleriyle belirlenir.

7.1.4. Kişisel veriler, ilgili mevzuatta öngörülen veya işleme amacının gerektirdiği süre boyunca muhafaza edilir. İşleme şartlarının ve saklama gerekliliğinin ortadan kalkması hâlinde kişisel veriler ilgili düzenlemelere uygun olarak silinir, yok edilir veya anonim hâle getirilir.

8. Veri İşleyenler, Üçüncü Taraflar ve Yurt Dışına Aktarım

8.1.1. Bahçeşehir Üniversitesi, faaliyetlerini yürütürken veri işleyenlerden, alt veri işleyenlerden, üçüncü taraf hizmet sağlayıcılardan ve bulut hizmet sağlayıcılarından hizmet alabilir.

8.1.2. Üniversite adına kişisel veri işleyen tarafların görev, yetki, gizlilik, güvenlik, veri ihlali bildirimi, alt veri işleyen kullanımı ve hizmetin sona ermesine ilişkin yükümlülükleri sözleşmelerle düzenlenir.

8.1.3. Üçüncü taraf hizmet sağlayıcılar, kişisel verilere erişim sağlamadan önce kurumsal uyum ve güvenlik değerlendirmesine tabi tutulur.

8.1.4. Kişisel verilerin yurt dışına aktarılması, KVKK’nın 9. maddesi ve ilgili ikincil mevzuat uyarınca; öncelikle Kişisel Verileri Koruma Kurulu tarafından verilen Yeterlilik Kararı’nın bulunması, Yeterlilik Kararı’nın bulunmaması hâlinde Uygun Güvencelerden (Standart Sözleşme, Bağlayıcı Şirket Kuralları vb.) birinin sağlanması veya kanunda sayılan arızi durum istisnalarının varlığı halinde gerçekleştirilir.

8.1.5. Üniversite bünyesinde kullanılan bulut ve dijital platformların verileri yurt dışındaki sunucularda barındırması durumunda, KVKK Madde 9'da öngörülen hukuki aktarım mekanizmaları tesis edilmeden ve gerekli güvenlik tedbirleri alınmadan söz konusu hizmetler kullanıma alınamaz.

9. Veri İhlalleri, Başvurular ve Şikâyetler

9.1.1. Kişisel verilerin yetkisiz kişilerce elde edilmesi, açıklanması, değiştirilmesi, kaybolması, erişilemez hâle gelmesi veya hukuka aykırı biçimde işlenmesi veri ihlali kapsamında değerlendirilir.

9.1.2. Veri ihlali veya veri ihlali şüphesi tespit edildiğinde durum, derhal ve gecikmeksizin yazılı olarak Bilgi İşlem Daire Başkanlığına ve Hukuk Müşavirliğine bildirilir.

9.1.3. Veri ihlallerinin teknik inceleme, erişim kısıtlama ve kök neden analizi süreçleri Bilgi İşlem Daire Başkanlığı; hukuki değerlendirme süreçleri ise Hukuk Müşavirliği tarafından koordineli biçimde yürütülür.

9.1.4. Veri ihlali bildirimleri ilgili mevzuatta öngörülen usul ve süreler içinde gerçekleştirilir. İlgili kişi başvuruları, veri ihlalleri, şikâyetler ve düzeltici faaliyetler kayıt altına alınır ve izlenir.

10. Yönetişim ve Sorumluluklar

10.1. Bu politikanın kurumsal sahibi Rektörlüktür. Rektörlük, kişisel verilerin korunmasına ilişkin üst yönetim gözetimini sağlar ve politikanın uygulanması için gerekli kurumsal koordinasyonun yürütülmesini gözetir.

10.2. Bilgi İşlem Daire Başkanlığı, politikanın günlük teknik ve operasyonel koordinasyonunu yürütür; kişisel veri güvenliği, bilgi sistemleri, Kişisel Veri İşleme Envanteri, teknik incelemeler, veri ihlalleri ve ilgili kişi başvurularının teknik boyutlarına ilişkin süreçleri koordine eder.

10.3. Hukuk Müşavirliği, Kişisel Verilerin Korunması Kanununa ilişkin hukuki değerlendirme ve uyum süreçlerini yürütür; ilgili kişi başvuruları, aydınlatma ve açık rıza metinleri, kişisel veri işleme ve aktarım sözleşmeleri, veri ihlali bildirimleri, yurt dışına aktarım ve uyuşmazlık süreçlerinin hukuki boyutlarını değerlendirir.

10.4. Akademik ve idari birimler, kendi görev alanlarındaki kişisel veri işleme faaliyetlerinin hukuka uygun, doğru, güncel, sınırlı ve ölçülü biçimde yürütülmesinden; süreçlere ilişkin bilgilerin Kişisel Veri İşleme Envanterine aktarılmasından ve ilgili birimlerle iş birliği yapılmasından sorumludur.

10.5. Birim yöneticileri; personelin politika ve ilgili düzenlemeler hakkında bilgilendirilmesini, görev ve erişim yetkilerinin güncel tutulmasını ve risk veya ihlallerin zamanında bildirilmesini sağlar.

10.6. Politika kapsamındaki tüm kişiler; kişisel verilere yalnızca yetkili oldukları faaliyetler kapsamında erişmek, kişisel verileri yetkisiz kişilerle paylaşmamak, Üniversitenin belirlediği güvenlik kurallarına uymak ve veri ihlali veya ihlal şüphesini gecikmeksizin bildirmekle yükümlüdür.

10.7. Gizlilik ve kişisel verilerin korunmasına ilişkin yükümlülükler, Üniversiteyle çalışma, öğrenim, proje veya hizmet ilişkisinin sona ermesinden sonra da devam eder.

11. Eğitim, İzleme ve Sürekli İyileştirme

11.1. Bahçeşehir Üniversitesi, kişisel verilerin korunmasına ilişkin kurumsal farkındalığın ve yetkinliğin geliştirilmesi amacıyla düzenli eğitim ve bilgilendirme çalışmaları yürütür.

11.2. Eğitimlerin kapsamı ve sıklığı; kişilerin görevleri, işledikleri veri türleri, erişim yetkileri ve faaliyetlerin taşıdığı riskler dikkate alınarak belirlenir.

11.3. Üniversite; Kişisel Veri İşleme Envanterini, ilgili kişi başvurularını, veri ihlallerini, saklama ve imha süreçlerini, üçüncü taraf ilişkilerini, yurt dışına veri aktarımlarını ve eğitim faaliyetlerini düzenli olarak izler ve değerlendirir.

11.4. İzleme, denetim, mevzuat değişiklikleri, kurumsal ihtiyaçlar ve uygulama deneyimleri doğrultusunda ilgili politikalar, prosedürler, sözleşmeler ve uygulama süreçleri güncellenir.

11.5. Politika ihlalleri, olayın niteliğine göre Üniversitenin öğrenci, personel, sözleşme, disiplin ve bilgi güvenliği düzenlemeleri çerçevesinde değerlendirilir.

12. Taahhüt, Yürürlük ve Uygulama

12.1 Bahçeşehir Üniversitesi, kişisel verilerin korunmasını kurumsal güvenin, akademik özgürlüğün, araştırma bütünlüğünün, öğrenci ve çalışan haklarının ve sorumlu üniversite yönetiminin temel koşullarından biri olarak kabul eder.

12.2. Üniversite; kişisel verilerin hukuka uygun, şeffaf, güvenli ve hesap verebilir biçimde işlenmesini, ilgili kişilerin haklarının korunmasını ve veri koruma kültürünün tüm akademik ve idari süreçlerde geliştirilmesini taahhüt eder.

12.3. Bu politika, Bahçeşehir Üniversitesi Senatosu tarafından onaylandığı tarihte yürürlüğe girer.

12.4. Bu politikanın kurumsal sahibi Rektörlüktür.

12.5. Politikanın günlük teknik ve operasyonel koordinasyonu Bilgi İşlem Daire Başkanlığı, Kişisel Verilerin Korunması Kanununa ilişkin hukuki değerlendirme süreçleri Hukuk Müşavirliği tarafından yürütülür.

12.6. Politika; mevzuat değişiklikleri, kişisel veri işleme faaliyetlerindeki gelişmeler, kurumsal ihtiyaçlar, denetim sonuçları ve uygulama deneyimleri doğrultusunda düzenli olarak gözden geçirilir.

12.7. Bu politika kapsamında ihtiyaç duyulan operasyonel ayrıntılar ve uygulama süreçleri, Üniversite tarafından geliştirilecek tamamlayıcı politika, yönerge, usul ve esas, prosedür, rehber, sözleşme ve diğer kurumsal düzenlemelerle belirlenebilir.

12.8. Bu politika ile Üniversitenin diğer düzenlemeleri arasında yorum farklılığı oluşması hâlinde yürürlükteki mevzuat, Senato kararları ve üst düzenleme niteliğindeki Üniversite politikaları esas alınır.

BAHÇEŞEHİR UNIVERSITY

PERSONAL DATA PROTECTION AND DATA PRIVACY POLICY

1. Purpose

Bahçeşehir University recognizes the protection of personal data as an integral element of individuals' fundamental rights and freedoms, the privacy of private life, institutional trust, and responsible data governance.

The purpose of this Policy is to establish the University's institutional approach, fundamental principles, duties, and responsibilities regarding the conduct of personal data processing activities within Bahçeşehir University in compliance with the Personal Data Protection Law No. 6698 and the relevant secondary legislation.

Bahçeşehir University adopts the principle that personal data shall be used lawfully, securely, transparently, accountably, and in a manner that is relevant, limited, and proportionate to the purposes for which they are processed in teaching and learning, research, societal contribution, administrative, academic, operational, and managerial processes.

This Policy establishes the University's high-level institutional framework for the protection of personal data. Operational, legal, and technical details relating to its implementation shall be governed by the University's relevant policies, procedures, directives, rules and principles, guidelines, agreements, and other institutional regulations.

2. Scope

2.1.

This Policy applies to personal data processing activities carried out by the legal entity of Bahçeşehir University in its capacity as a data controller or data processor.

This Policy applies to:

a) Full-time and part-time academic staff,
b) Administrative staff,
c) Students and alumni,
ç) Prospective students,
d) Researchers and project personnel,
e) Visiting academics and researchers,
f) Interns and scholarship holders,
g) Consultants,
ğ) Service provider and subcontractor personnel providing services on behalf of the University,
h) External participants in committee, board, and jury activities,
ı) Campus visitors,
i) Other natural and legal persons carrying out activities on behalf of the University or using data belonging to the University.

2.2.

This Policy applies where students access or use personal data belonging to Bahçeşehir University or processed by the University within the scope of education, research, projects, internships, practical activities, societal contribution, or other activities.

2.3.

Pursuant to Article 28(1)(a) of the Personal Data Protection Law, personal data processing activities carried out by individuals solely in relation to themselves or family members living in the same household are outside the scope of this Policy.

However, the processing by such individuals, outside their institutional purposes and authority, of personal data for which the University is the data controller or to which they have access within the scope of University processes constitutes a violation of this Policy and the relevant institutional regulations.

2.4.

Organizations with separate legal personality are not directly covered by this Policy. In activities conducted with such organizations, the parties' capacities as data controller or data processor shall be determined according to the nature of the personal data processing activity and regulated through the necessary agreements.

3. Fundamental Approach and Principles

Bahçeşehir University does not regard the protection of personal data solely as an information technology or legal compliance matter. Personal data protection is an area of institutional governance requiring shared responsibility across all academic and administrative processes of the University.

Bahçeşehir University adopts the following fundamental principles in the processing of personal data:

3.1. Lawfulness and Fairness

Personal data shall be processed in compliance with the Personal Data Protection Law, the relevant secondary legislation, and the University's institutional regulations. The rights and reasonable expectations of data subjects shall be respected in personal data processing activities.

3.2. Accuracy and Currency

Personal data shall be accurate and, where necessary, kept up to date. The necessary processes shall be implemented to rectify personal data identified as incomplete or inaccurate.

3.3. Processing for Specified, Explicit, and Legitimate Purposes

Personal data shall be processed for predetermined, explicit, and legitimate purposes. Personal data shall not be used in a manner incompatible with the purposes for which they were collected.

3.4. Relevance, Limitation, and Proportionality to the Purpose of Processing

Personal data shall be collected, used, and retained only to the extent required for the purpose of processing. Access to personal data shall be limited according to duties, authority, and institutional requirements.

3.5. Retention for the Necessary Period

Personal data shall be retained for the period prescribed by the relevant legislation or required by the purpose of processing. Personal data whose retention period has expired shall be deleted, destroyed, or anonymized in accordance with the relevant institutional regulations.

3.6. Transparency

Data subjects shall be informed in a clear and understandable manner about the purposes and legal grounds of personal data processing, the methods of collection, and the recipient groups to which their personal data may be transferred.

3.7. Accountability

The University shall establish and maintain up-to-date records, inventories, agreements, and other institutional documents demonstrating that its personal data processing activities comply with the Personal Data Protection Law and the relevant institutional regulations.

3.8. Confidentiality, Integrity, and Availability

Appropriate technical and administrative measures shall be taken to protect personal data against unauthorized access, disclosure, alteration, loss, corruption, or destruction.

This Policy is not a privacy notice. Privacy notices relating to specific personal data processing activities shall be prepared separately, based on the nature of the relevant activity and the current information contained in the Personal Data Processing Inventory.

4. Processing of Personal Data and the Personal Data Processing Inventory

4.1.

Bahçeşehir University shall process personal data only where at least one of the personal data processing conditions or legal grounds set out in the Personal Data Protection Law exists.

4.2.

Explicit consent is not the sole or default legal ground for processing personal data. Where a processing activity may rely on another legal ground, the relevant processing condition shall be applied. Explicit consent shall be obtained only where required by the nature of the activity or the applicable legislation.

4.3.

The University’s personal data processing activities shall be recorded in the Personal Data Processing Inventory. The Inventory constitutes the primary source for privacy notices, retention and disposal processes, data transfer arrangements, and other institutional personal data management practices.

4.4.

Academic and administrative units shall contribute to ensuring that the personal data processing activities within their respective areas of responsibility are accurately and currently reflected in the Inventory.

4.5.

New or substantially modified data processing activities, systems, software, digital platforms, research projects, artificial intelligence applications, and outsourced services shall be assessed in terms of the applicable legislation, information security, and institutional responsibilities before they are put into use.

5. Rights of Data Subjects

5.1.

All rights granted to data subjects under the Personal Data Protection Law No. 6698 and the relevant legislation are reserved.

5.2.

Data subjects may exercise their rights concerning the processing of their personal data by applying to the University in accordance with the procedures and principles prescribed by the applicable legislation.

5.3.

Applications may be submitted through kvkk@bau.edu.tr or through other application channels announced by the University.

5.4.

The legal assessment of and response to data subject applications shall be coordinated by the Office of Legal Counsel on behalf of the Data Controller. The Information Technologies Department and the relevant academic or administrative units shall provide the necessary information and documentation for technical verification, examination of system records, and the conduct of operational processes.

5.5.

Applications shall be concluded within the procedures and time limits prescribed by the applicable legislation.

6. Protection of Personal Data in University Activities

6.1. Teaching and Learning Processes

6.1.1.

Students’ personal data shall be processed for the purposes of carrying out registration, teaching and learning, assessment and evaluation, academic advising, support services, internships, graduation, and other academic processes, and only to the extent required for such processes.

6.1.2.

Student data shall not be disclosed to unauthorized persons, used outside institutional purposes, or transferred to systems not approved by the University.

6.1.3.

Academic staff and students shall comply with personal data protection obligations in courses, examinations, assignments, projects, theses, internships, and other academic activities.

6.2. Research Processes

6.2.1.

Personal data used in research activities shall be processed in accordance with scientific ethics, research integrity, data subject rights, data security requirements, and the necessary ethics committee processes.

6.2.2.

Principal investigators shall be responsible for the lawfulness, security, access authorizations, and retention of personal data processed within the scope of research, as well as the actions to be taken upon completion of the research.

6.2.3.

In collaborative research activities, the capacities of the parties as data controller or data processor and their respective duties and obligations concerning personal data shall be determined by agreements.

6.3. Administrative, Operational, and Managerial Processes

6.3.1.

Personal data relating to employees, students, alumni, prospective students, visitors, suppliers, and other data subjects may be processed for the purposes of carrying out the University’s human resources, student services, financial affairs, security, communications, contract management, quality assurance, and other institutional activities.

6.3.2.

Personal data shall be used only by authorized persons and solely within the scope of their duties. In academic, administrative, and managerial decisions that significantly affect individuals, final assessment and responsibility shall remain with the authorized persons.

6.4. Sensitive Data and Activities Requiring Special Protection

6.4.1.

Stricter technical, administrative, and legal measures shall be applied to the processing of sensitive data and to personal data processing activities that may have a significant impact on individuals’ fundamental rights and freedoms.

6.4.2.

Access to sensitive data shall be restricted to authorized persons whose duties require such access.

6.4.3.

Comprehensive monitoring, profiling, analysis conducted exclusively through automated systems, large-scale data processing, and similar activities shall be subject to assessment by the relevant institutional units before implementation.

7. Data Security, Retention, and Disposal

7.1.1.

Bahçeşehir University shall take the necessary technical and administrative measures to ensure an appropriate level of security in order to prevent unlawful processing of or unlawful access to personal data and to ensure the secure retention of personal data.

7.1.2.

The confidentiality, integrity, and availability of personal data shall be protected through role- and authorization-based access, institutional information security practices, and appropriate recording and monitoring mechanisms.

7.1.3.

Technical and operational security measures shall be governed by the University's regulations concerning information security, access, devices, networks, databases, suppliers, retention, and disposal.

7.1.4.

Personal data shall be retained for the period prescribed by the applicable legislation or required by the purpose of processing. Where the conditions for processing and the need for retention cease to exist, personal data shall be deleted, destroyed, or anonymized in accordance with the relevant regulations.

8. Data Processors, Third Parties, and International Transfers

8.1.1.

Bahçeşehir University may obtain services from data processors, sub-processors, third-party service providers, and cloud service providers in the course of its activities.

8.1.2.

The duties, authority, confidentiality and security obligations, personal data breach notification requirements, use of sub-processors, and end-of-service obligations of parties processing personal data on behalf of the University shall be regulated by agreements.

8.1.3.

Third-party service providers shall undergo institutional compliance and security assessments before being granted access to personal data.

8.1.4.

Pursuant to Article 9 of the Personal Data Protection Law and the relevant secondary legislation, personal data may be transferred abroad where an Adequacy Decision issued by the Personal Data Protection Board exists; where no Adequacy Decision exists, where one of

the Appropriate Safeguards, including a Standard Contract or Binding Corporate Rules, has been established; or where one of the exceptional circumstances for occasional transfers specified by law applies.

8.1.5.

Where cloud or digital platforms used by the University store data on servers located abroad, such services shall not be put into use unless the legal transfer mechanisms prescribed under Article 9 of the Personal Data Protection Law have been established and the necessary security measures have been implemented.

9. Personal Data Breaches, Applications, and Complaints

9.1.1.

Unauthorized acquisition, disclosure, alteration, loss, unavailability, or unlawful processing of personal data shall be considered a personal data breach.

9.1.2.

Where a personal data breach or a suspected breach is identified, it shall be reported immediately and without delay, in writing, to the Information Technologies Department and the Office of Legal Counsel.

9.1.3.

Technical investigation, access restriction, and root-cause analysis relating to personal data breaches shall be carried out by the Information Technologies Department, while legal assessment processes shall be carried out by the Office of Legal Counsel in coordination with the relevant units.

9.1.4.

Personal data breach notifications shall be made in accordance with the procedures and time limits prescribed by the applicable legislation. Data subject applications, personal data breaches, complaints, and corrective actions shall be recorded and monitored.

10. Governance and Responsibilities

10.1.

The Rectorate is the institutional owner of this Policy. The Rectorate shall provide senior management oversight regarding the protection of personal data and oversee the institutional coordination necessary for the implementation of this Policy.

10.2.

The Information Technologies Department shall carry out the daily technical and operational coordination of the Policy and coordinate processes relating to personal data security, information systems, the Personal Data Processing Inventory, technical examinations, personal data breaches, and the technical aspects of data subject applications.

10.3.

The Office of Legal Counsel shall carry out legal assessment and compliance processes relating to the Personal Data Protection Law and assess the legal aspects of data subject applications, privacy notices and explicit consent texts, personal data processing and transfer agreements, personal data breach notifications, international transfers, and disputes.

10.4.

Academic and administrative units shall be responsible for ensuring that personal data processing activities within their areas of responsibility are conducted lawfully, accurately, currently, in a limited and proportionate manner; for providing the information necessary for inclusion in the Personal Data Processing Inventory; and for cooperating with the relevant units.

10.5.

Unit managers shall ensure that personnel are informed about this Policy and the relevant regulations, that duties and access authorizations are kept up to date, and that risks or breaches are reported in a timely manner.

10.6.

All persons covered by this Policy shall access personal data only within the scope of the activities for which they are authorized, refrain from sharing personal data with unauthorized persons, comply with the security rules established by the University, and report any personal data breach or suspected breach without delay.

10.7.

Obligations relating to confidentiality and the protection of personal data shall continue after the termination of an individual’s employment, education, project, or service relationship with the University.

11. Training, Monitoring, and Continuous Improvement

11.1.

Bahçeşehir University shall conduct regular training and informational activities to enhance institutional awareness and competence regarding the protection of personal data.

11.2.

The scope and frequency of training shall be determined by considering individuals’ duties, the types of data they process, their access authorizations, and the risks associated with their activities.

11.3.

The University shall regularly monitor and evaluate the Personal Data Processing Inventory, data subject applications, personal data breaches, retention and disposal processes, third-party relationships, international data transfers, and training activities.

11.4.

Relevant policies, procedures, agreements, and implementation processes shall be updated in light of monitoring and audit findings, legislative changes, institutional requirements, and implementation experience.

11.5.

Violations of this Policy shall be assessed, depending on the nature of the incident, within the framework of the University's student, personnel, contractual, disciplinary, and information security regulations.

12. Commitment, Entry into Force, and Implementation

12.1.

Bahçeşehir University recognizes the protection of personal data as one of the fundamental conditions of institutional trust, academic freedom, research integrity, student and employee rights, and responsible university governance.

12.2.

The University is committed to ensuring that personal data are processed lawfully, transparently, securely, and accountably; that the rights of data subjects are protected; and that a culture of data protection is developed across all academic and administrative processes.

12.3.

This Policy shall enter into force on the date of its approval by the Senate of Bahçeşehir University.

12.4.

The Rectorate is the institutional owner of this Policy.

12.5.

The daily technical and operational coordination of the Policy shall be carried out by the Information Technologies Department, while legal assessment processes relating to the Personal Data Protection Law shall be carried out by the Office of Legal Counsel.

12.6.

This Policy shall be reviewed regularly in light of legislative amendments, developments in personal data processing activities, institutional requirements, audit findings, and implementation experience.

12.7.

Operational details and implementation processes required under this Policy may be governed by supplementary policies, directives, rules and principles, procedures, guidelines, agreements, and other institutional regulations to be developed by the University.

12.8.

Where an inconsistency of interpretation arises between this Policy and other University regulations, the applicable legislation, Senate resolutions, and superior University policies shall prevail.