|  |  |  |
| --- | --- | --- |
| ID | SOURCE | TARGET |
| [Screen 0](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=1_C_1) [1\_C\_1](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=1_C_1)  | Protecting Sensitive DataClick the forward arrow to begin. | Hassas Verilerin KorunmasıBaşlamak için ileri okuna tıklayın. |
| [Screen 1](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=2_C_2) [2\_C\_2](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=2_C_2)  | At Abbott, we rely on data to make decisions - often that data contains sensitive information.For us to fulfill our mission of helping people live their best lives through good health, it is essential that we keep this data secure and comply with the laws and ethical standards that Abbott upholds. This course is designed to give you the skills needed to support this task. | Abbott’ta karar vermek için verilere dayanırız - bu veriler sıklıkla hassas bilgiler içerir.İnsanlara iyi sağlık sayesinde en iyi hayatlarını yaşamalarına yardımcı olma misyonumuzu yerine getirmemiz için bu verileri güvende tutmamız ve yasalara ve Abbott’ın desteklediği etik standartlara uymamız temel önem taşır. Bu kurs bu beceriyi desteklemek için gereken becerileri size kazandırmak için tasarlanmıştır. |
| [Screen 2](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=3_C_3) [3\_C\_3](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=3_C_3)  | After completing this course, you will have a better understanding of:* What sensitive data is,
* How we protect this data at Abbott,
* Your role in protecting sensitive data, and
* What to do if you think sensitive data may have been improperly disclosed or compromised.
 | Bu kursu tamamladıktan sonra şunlar hakkında daha iyi bir anlayışa sahip olacaksınız:* Hassas veri nedir,
* Bu verileri Abbott’ta nasıl koruruz,
* Hassas verilerin korunmasında sizin rolünüz ve
* Hassas verilerin uygunsuz şekilde açıklanmış veya tehlikeye girmiş olabileceğini düşündüğünüz takdirde ne yapılmalıdır.
 |
| [Screen 3](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=4_C_4) [4\_C\_4](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=4_C_4)  | 1 | Personal InformationHere you will learn how governments, consumers, and the public have become increasingly concerned about the privacy and security of personal information.12 MinutesSection 1 | Personal InformationRecognizing Personal InformationLegal, Regulatory and Contractual RequirementsAbbott’s Privacy by Design PrinciplesReview2 | Confidential Business InformationHere you will learn how most of the business information we use in our day-to-day work activities is considered confidential.5 MinutesSection 2 | Confidential Business InformationRecognizing Confidential Business InformationCost of Not Protecting Confidential Business InformationInsider InformationReview3 | Protecting Sensitive DataHere you will learn what you can do to help protect sensitive data.8 MinutesSection 3 | Your Role in Protecting Sensitive DataAccessing and Using Sensitive DataSharing Sensitive DataRetaining and Disposing of Sensitive DataResponding to Improper DisclosuresReview4 | Knowledge CheckAssess your understanding of the key concepts and principles of this course.5 MinutesSection 4 | Knowledge CheckAssessmentClick the panel to get started.Click the yellow play button to begin.This content is not yet available. You must complete Section{a} {b}. | 1 | Kişisel BilgilerBurada, son yıllarda devletlerin, tüketicilerin ve toplumun kişisel bilgilerin gizliliği ve güvenliği konusunda nasıl giderek daha fazla endişe duyar duruma geldiğini öğreneceksiniz.12 DakikaBölüm 1 | Kişisel BilgilerKişisel Bilgileri TanımaYasal, Düzenleyici ve Sözleşme GereklilikleriAbbott’ın Tasarım itibarıyla Gizlilik İlkeleriİncele2 | Gizli Ticari BilgilerBurada, günlük iş faaliyetlerimizde kullandığımız ticari bilgilerin çoğunun nasıl gizli kabul edildiğini öğreneceksiniz.5 DakikaBölüm 2 | Gizli Ticari BilgilerGizli Ticari Bilgileri TanımaGizli Ticari Bilgilerin Korunmamasının Maliyetiİçeriden Bilgiİncele3 | Hassas Verilerin KorunmasıBurada, hassas verilerin korunmasına yardımcı olmak için ne yapabileceğinizi öğreneceksiniz.8 DakikaBölüm 3 | Hassas Bilgilerin Korunmasındaki RolünüzHassas Verilere Erişim ve KullanımHassas Verilerin PaylaşılmasıHassas Verilerin Saklanması ve İmhasıUygunsuz İfşalara Müdahaleİncele4 | Bilgi KontrolüBu kursun temel kavramları ve ilkeleri hakkındaki anlayışınızı değerlendirin.5 DakikaBölüm 4 | Bilgi KontrolüDeğerlendirmeBaşlamak için panele tıklayın.Başlamak için sarı oynatma düğmesine tıklayın.Bu içerik henüz mevcut değil. Bölüm{a} {b}’yi tamamlamak zorundasınız. |
| [Screen 4](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=5_C_7) [5\_C\_7](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=5_C_7)  | At Abbott, one common type of sensitive data we use is personal information.In recent years, governments, consumers, and the general public have become increasingly concerned about the privacy and security of personal information. | Abbott’ta, kullandığımız yaygın bir hassas veri türü kişisel bilgidir.Son yıllarda, devletler, tüketiciler ve kamu, kişisel bilgilerin gizliliği ve güvenliği konusunda giderek daha fazla endişe duymaya başlamıştır. |
| [Screen 5](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=6_C_8) [6\_C\_8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=6_C_8)  | Personal information is any information that can be used to contact, locate, or otherwise identify an individual. | Kişisel bilgiler, bir kişiyle iletişim kurmak, bulunduğu yeri belirlemek veya onu tanımlamak için kullanılabilecek her türlü bilgilerdir. |
| [Screen 6](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=7_C_9) [7\_C\_9](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=7_C_9)  | Kandice | Marketing Manager Can you give me some examples of personal information?Personal information can include biographical information, such as name, date of birth, email address and phone number.It can include information relating to an individual’s appearance, such as hair color or weight.It can also include information relating to an individual’s personal life, such as photos, browser cookies or location tracking information. | Kandice | Pazarlama Müdürü Bana bazı kişisel bilgi örnekleri verebilir misiniz?Kişisel bilgiler isim, doğum tarihi, e-posta adresi ve telefon numarası gibi biyografik bilgileri içerebilir.Bunlar, saç rengi veya kilo gibi bir kişinin görünümüyle ilgili bilgileri içerebilir.Bunlar, fotoğraflar, tarayıcı tanımlama bilgileri veya konum izleme bilgileri gibi bireyin kişisel hayatıyla ilgili bilgileri de içerebilir. |
| [Screen 7](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=8_C_10) [8\_C\_10](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=8_C_10)  | Jerry | Sales Representative Does personal information also include protected health information?Yes, it does.Protected health information (PHI) is a particularly sensitive type of personal information used in the healthcare industry. It includes any personally identifiable information in medical records, including conversations between medical professionals about treatment. | Jerry | Satış Temsilcisi Kişisel bilgiler kapsamına korunan sağlık bilgileri de girer mi?Evet, girer.Korunan sağlık bilgileri (PHI), sağlık hizmetleri sektöründe kullanılan, özellikle hassas bir kişisel bilgi türüdür. Tıp uzmanları arasındaki tedavi üzerine konuşmalar da dahil olmak üzere, tıbbi kayıtlarda yer alan kişiyi tanımlamak için kullanılabilecek her türlü bilgiyi içerir. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=9_C_11) [9\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=9_C_11)  | In most countries in which Abbott conducts business, there are laws and regulations in place designed to protect personal information, including protected health information.Laws relating to privacy and protection of personal information differ from one country to the next, but often embrace the same core principles.CLICK EACH OF THE HIGHLIGHTED AREAS ONSCREEN TO LEARN ABOUT THE DIFFERENT TYPES OF PRIVACY LAWS AND REQUIREMENTS IN PLACE AROUND THE WORLD. | Abbott’ın faaliyet gösterdiği çoğu ülkede, korunan sağlık bilgileri dahil olmak üzere, kişisel bilgileri korumak için tasarlanmış yasa ve düzenlemeler bulunmaktadır.Kişisel bilgilerin gizliliği ve korunması ile ilgili bilgiler bir ülkeden diğerine farklılık gösterir, ama genellikle aynı temel ilkeleri benimserler.DÜNYANIN ÇEŞİTLİ YERLERİNDE YÜRÜRLÜKTE OLAN FARKLI TÜRDEN YASALAR VE GEREKLİLİKLER HAKKINDA BİLGİ EDİNMEK İÇİN EKRANDAKİ İŞARETLENMİŞ ALANLARIN HER BİRİNE TIKLAYIN. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=10_C_11) [10\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=10_C_11)  | EuropeIn Europe, the General Data Protection Regulation (GDPR) is one of the most comprehensive privacy laws globally, and since its implementation in 2018, it has set the standard for privacy protection that other countries are trying to emulate. GDPR applies to organizations located within Europe, as well as organizations located outside of Europe that offer goods and services to or monitor the behavior of any individual residing in Europe.One of the key concepts of GDPR is the right to erasure, also known as the right to be forgotten. This right gives individuals the ability to request that their personal data be erased from an organization's records. If an individual makes such a request, the organization must take steps to erase the data from its systems and prevent its further use or disclosure. There may be exceptions to data subject requests. Nonetheless, Abbott will inform each validated data subject of what action is taken for each request. Violations of GDPR can result in heavy fines for companies, up to 4% of their annual global turnover, or 20 million euros (whichever is greater), for the most serious offenses. | AvrupaAvrupa Genel Veri Koruma Düzenlemesi (GDPR), küresel olarak en kapsamlı gizlilik yasalarından biridir ve 2018 yılında uygulanmasından beri, diğer ülkelerin aynı düzeye ulaşmaya çalıştığı gizlilik koruması standardını belirlemiştir. GDPR, Avrupa’da yerleşik olan kuruluşların yanı sıra Avrupa dışında yerleşik olan ve Avrupa’da yerleşik herhangi bir bireye ürünler ve hizmetler sunan veya onun davranışlarını izleyen kuruluşlar için geçerlidir.GDPR’nin temel kavramlarından birisi, unutulma hakkı olarak da bilinen silinme hakkıdır. Bu hak, bireylere, kişisel verilerinin bir kuruluşun kayıtlarından silinmesini talep etme yeteneği vermektedir. Bir bireyin böyle bir talepte bulunması durumunda, kuruluş, verileri kendi sistemlerinden silmek ve bunların daha fazla kullanılmasını veya açıklanmasını önlemek için adımlar atmak zorundadır. Veri sahibi talepleri için istisnalar bulunabilir. Yine de, Abbott, doğrulanmış her veri sahibine her talep için ne önlem alındığı hakkında bilgi verecektir. GDPR ihlalleri, en ağır suçlar için, şirketler için yıllık küresel cirolarının %4’üne veya 20 milyon avroya (hangisi daha büyükse) kadar varan ağır para cezaları ile sonuçlanabilir. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=11_C_11) [11\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=11_C_11)  | United StatesIn the United States, there is no single law that protects all personal information. Instead, there are privacy laws and regulations that apply to specific industries and types of data. For example, HIPAA protects the privacy of healthcare data, while the Fair Credit Reporting Act protects credit information.However, some states have begun enacting their own comprehensive data privacy laws. For instance, California has the California Consumer Privacy Act (CCPA), which gives Californians certain rights to their data, such as the right to know what personal information is being collected about them and the right to delete any personal information collected. The CCPA will be amended by the California Privacy Rights Act (CPRA) in 2023, which will give people even more rights to their data.Other states that have passed their own data privacy laws include Virginia, Colorado, Utah, and Connecticut. While each state's law is different, they all generally give people rights to their data and require companies to provide certain disclosures about their data processing activities.Fines for violating state privacy laws can be significant. For example, California can fine companies up to $7,500 USD per violation of the CCPA.CanadaThere are laws at both the federal and provincial levels in Canada that are designed to protect an individual's personal information. For example, the Personal Information Protection and Electronic Documents Act (PIPEDA) is a federal law that applies to private sector organizations and is enforced by the Office of the Privacy Commissioner of Canada.At the provincial level, Quebec, Alberta, and British Columbia have enacted privacy laws that are similar to PIPEDA. Some other provinces also have rules in place that provide similar protections for personal information, including the provinces of Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia, which have enacted health information privacy laws.These laws are in place to help prevent personal information from being mishandled or collected without the individual's knowledge, and give people the right to access their own information and correct any errors.Violating these laws can result in significant fines. For example, violating PIPEDA can lead to a fine of up to $100,000. In Alberta, the Personal Information Protection Act (PIPA) allows for fines of up to $10,000 for individuals and $500,000 for organizations. | Amerika Birleşik DevletleriAmerika Birleşik Devletleri’nde tüm kişisel bilgileri koruyan tek bir yasa yoktur. Bunun yerine, belirli endüstriler ve veri türleri için geçerli olan gizlilik yasaları ve düzenlemeleri bulunmaktadır. Örneğin, HIPAA sağlık hizmeti verilerinin gizliliğini korurken Adil Kredi Raporlama Yasası kredi bilgilerini korumaktadır.Ama bazı eyaletler kendi geniş kapsamlı veri gizliliği yasalarını yasalaştırmaya başlamıştır. Örneğin Kaliforniya’da Kaliforniya Tüketici Gizliliği Yasası (CCPA) bulunmaktadır ve Kaliforniyalılara, kendileri hakkında hangi kişisel bilgilerin toplanmakta olduğunu bilme hakkı ve toplanan herhangi bir kişisel bilgiyi silme hakkı gibi kendi verileri üzerinde bazı haklar vermektedir. CCPA 2023 yılında, insanlara kendi verileri üzerinde daha da çok hak verecek olan Kaliforniya Gizlilik Hakları Yasası (CPRA) ile değiştirilecektir.Kendi veri gizliliği yasalarını geçirmiş olan diğer eyaletler arasında Virginia, Colorado, Utah ve Connecticut bulunmaktadır. Her eyaletin yasası farklı olmasına karşın bunların hepsi genel olarak insanlara kendi verileri üzerinde haklar vermekte ve şirketlerin kendi veri işleme faaliyetleri hakkında bazı açıklamalar sağlamasını gerekli tutmaktadır.Eyalet gizlilik yasalarının ihlal edilmesi yüzünden para cezaları çok büyük olabilir. Örneğin Kaliforniya, CCPA’nın her ihlali için şirketlere 7.500 ABD$ tutarına kadar para cezası uygulayabilir.KanadaKanada’da bireylerin kişisel bilgilerini korumak için tasarlanmış olan hem federal düzeyde hem eyalet düzeyinde yasalar bulunmaktadır. Örneğin, Kişisel Bilgi Koruması ve Elektronik Belgeler Yasası (PIPEDA), özel sektör kuruluşları için geçerli olan federal bir yasadır ve Kanada Gizlilik Komiserliği tarafından yürütülmektedir.Eyalet düzeyinde, Quebec, Alberta ve British Columbia, PIPEDA’ya benzer olan gizlilik yasaları yasalaştırmıştır. Ontario, New Brunswick, Newfoundland and Labrador ve Nova Scotia eyaletleri dâhil olmak üzere bazı başka eyaletler de kişisel bilgiler için benzer koruma önlemleri sağlayan kurallara sahiptir ve bunlar sağlık bilgileri gizlilik yasalarını yasalaştırmıştır.Bu yasalar, kişisel bilgilerin kötü şekilde ele alınmasını veya bireyin bilgisi olmadan toplanmasını önlemeye yardımcı olmak için mevcut bulunmaktadır ve insanlara kendi bilgilerine erişme ve herhangi bir yanlışlığı düzeltme hakkı vermektedir.Bu yasaların ihlal edilmesi büyük para cezaları ile sonuçlanabilir. Örneğin PIPEDA’nın ihlal edilmesi 100.000 ABD$ tutarına kadar bir para cezasına yol açabilir. Alberta’da, Kişisel Bilgi Koruması Yasası (PIPA), bireyleri için 10.000 ABD$ tutarına kadar ve kuruluşlar için 500.000 ABD$ tutarına kadar para cezalarına olanak vermektedir. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=12_C_11) [12\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=12_C_11)  | Asia PacificThe privacy laws in the Asia Pacific region are constantly expanding and becoming more comprehensive. Some countries, such as China, have implemented data localization measures which require companies to store some personal data on servers within their borders. Additionally, China has privacy and security impact assessment requirements for the cross-border transfer of personal information.Others, like Australia and Singapore, have adopted a more consumer-focused approach to privacy that gives individuals greater control over their information, including the right to know how companies are using it and the ability to access and correct it if necessary.The penalties for companies who violate data privacy laws also differ widely across the region. In China, for example, companies can be fined up to 500,000 RMB (about $72,000 USD) for violating data privacy laws.However, in Singapore, companies can be fined up to 1 million (Singapore) dollars (about $737,000 USD) for violating the country’s privacy law. | Asya PasifikAsya Pasifik bölgesindeki gizlilik yasaları sürekli genişlemekte ve daha kapsamlı duruma gelmektedir. Çin gibi bazı ülkeler, şirketlerin bazı kişisel verileri kendi sınırları içindeki sunucularda depolamasını gerekli tutan veri yerelleştirme önlemleri uygulamıştır. Ek olarak, Çin, kişisel bilgilerin sınır ötesi aktarımı için gizlilik ve güvenlik etki değerlendirmesi gerekliliklerine sahiptir.Avustralya ve Singapur gibi başka ülkeler, gizlilik konusunda, bireylere kendi bilgileri üzerinde daha geniş bir kontrol veren daha tüketici odaklı bir yaklaşım benimsemiştir ve şirketlerin bu bilgileri nasıl kullandığını bilme hakkı ve gerekli ise bunlara erişme ve bunları silme yeteneği buna dâhildir.Veri gizliliği yasalarını ihlal eden şirketler için cezalar da bölge içinde geniş şekilde farklılık göstermektedir. Örneğin Çin’de, veri gizliliği yasalarını ihlal etmek yüzünden şirketlere 500.000 RMB (yaklaşık 72.000 ABD$) tutarına kadar para cezası verilebilir.Ama Singapur’da, ülkenin gizlilik yasasını ihlal etmek yüzünden şirketlere 1 milyon (Singapur) doları (yaklaşık 737.000 ABD$) tutarına kadar para cezası verilebilir. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=13_C_11) [13\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=13_C_11)  | RussiaRussia also has laws to protect its citizens' data, including a data localization law, which requires companies to store the personal data of Russian citizens on servers located in Russia.The law applies to companies that process the data of Russia's citizens, regardless of whether those companies are based in Russia or not. So, for example, a U.S.-based company that processes the data of Russian citizens would need to comply with the law.Like many countries, the law also requires companies to take steps to protect the personal data they process. For example, companies must ensure that the data is accurate and up-to-date and take steps to prevent it from being mishandled, lost, or stolen.The fines for violating the law can range from $12,000 to $72,000 USD for the first offense and up to $216,000 USD for the second offense. | RusyaRusya da vatandaşlarının verilerini korumak için, şirketlerin Rus vatandaşlarının kişisel verilerini Rusya’da bulunan sunucularda depolamasını gerekli tutan veri yerelleştirme yasası dâhil yasalara sahiptir.Bu yasa, Rus vatandaşlarının verilerini işleyen şirketlerin Rusya’da yerleşik olup olmadığına bakılmaksızın bu şirketler için geçerlidir. Örneğin, Rus vatandaşlarının verilerini işleyen A.B.D.’de yerleşik bir şirketin bu yasaya uyması gerekecektir.Birçok ülke gibi bu yasa da şirketlerin işledikleri kişisel verileri korumak için adımlar atmasını da gerektirmektedir. Örneğin şirketler verilerin doğru ve güncel olmasını sağlamak ve bunların kötü şekilde ele alınmasını, kaybolmasını veya çalınmasını önlemek için adımlar atmak zorundadır.Yasanın ihlal edilmesi yüzünden para cezaları birinci suçta 12.000 ABD$ ila 72.000 ABD$ arasında ve ikinci suçta 216.000 ABD$ tutarına kadar değişebilmektedir. |
| [Screen 8](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=14_C_11) [14\_C\_11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=14_C_11)  | Latin AmericaMost Latin American countries have laws in place that protect the privacy of individuals. However, many countries in the region, such as Ecuador, Argentina and Brazil, have recently revised their existing privacy regulations to stay current with international standards.Ecuador, for example, recently passed the Organic Law on the Protection of Personal Data (LPPD), which will go into effect in 2023. This law applies to any company around the world that processes the personal data of individuals in Ecuador.Like others in the region, the LPPD requires companies to provide notice and collect consent from individuals before using their data, destroy it when it is no longer needed, and meet certain restrictions before data is shared with other countries. These measures help protect the privacy of individuals across Latin America and ensure that companies are handling personal data responsibly.Violations of the LPPD can result in significant fines, ranging from 3% to 17% of an organization’s annual revenue from the previous year, providing a strong incentive for companies to comply with the law. | Latin AmerikaLatin Amerika ülkelerinin çoğu bireylerin gizliliğini koruyan yasalara sahiptir. Ama Ekvator, Arjantin ve Brezilya gibi bölgedeki birçok ülke uluslararası standartlara uygun durumda olmak için mevcut gizlilik düzenlemelerini kısa süre önce revize etmiştir.Örneğin Ekvator kısa süre önce, 2023 yılında yürürlüğe girecek olan Kişisel Verilerin Korunması hakkında Organik Yasayı (LPPD) geçirmiştir. Bu yasa, Ekvator’daki bireylerin kişisel verilerini işleyen dünyanın çeşitli yerlerindeki herhangi bir şirket için geçerlidir.Bölgedeki diğerleri gibi LPPD de şirketlerin bireylerin verilerini kullanmadan önce onlara bildirimde bulunmalarını ve onlardan müsaade almalarını, artık gerekli olmadıklarında bunları imha etmelerini ve veriler başka ülkeler ile paylaşılmadan önce bazı kısıtlamalara uymalarını gerektirmektedir. Bu önlemler tüm Latin Amerika’daki bireylerin gizliliğinin korunmasına yardımcı olmakta ve şirketlerin kişisel verileri sorumlu şekilde ele almasını sağlamaktadır.LPPD’nin ihlalleri, bir kuruluşun önceki yıldan gelen yıllık gelirinin %3 ila %17’si arasında değişen büyük para cezaları ile sonuçlanabilir ve bu, şirketlerin yasaya uyması için güçlü bir güdü sağlamaktadır. |
| [Screen 9](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=15_C_12) [15\_C\_12](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=15_C_12)  | In addition to laws and regulations governing how Abbott conducts business, there may be additional obligations in specific contracts we have with customers.For example, the U.S. government is a customer of Abbott. Under the terms of such an agreement, we are required to meet the obligations set out in the U.S. Privacy Act of 1974.CLICK THE ‘PRIVACY ACT’ BUTTON TO LEARN MORE. | Abbott’ın işlerini yürütme şeklini düzenleyen yasa ve düzenlemelere ek olarak, müşterilerimizle yaptığımız spesifik sözleşmelerde de ek yükümlülükler bulunabilir.Örneğin, ABD hükümeti Abbott’ın bir müşterisidir. Bu tür bir anlaşmanın şartları uyarınca, 1974 tarihli ABD Gizlilik Yasasında belirtilen yükümlülükleri yerine getirmemiz gereklidir.DAHA FAZLA BİLGİ İÇİN ‘GİZLİLİK YASASI’ DÜĞMESİNİ TIKLAYIN. |
| [Screen 9](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=16_C_12) [16\_C\_12](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=16_C_12)  | Privacy ActThe Privacy Act of 1974 (5 U.S.C. 552a) is an important Federal regulation. It establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals maintained in systems of records by federal agencies. For certain transactions, Abbott may be granted access to government agency records. In such cases, Abbott must meet several obligations, including the need to demonstrate that privacy training on protecting personally identifiable information has been conducted.Employees should contact Legal before entering into any agreements with customers that have privacy obligations. | Gizlilik Yasası1974 tarihli Gizlilik Yasası (5 U.S.C. 552a) önemli bir Federal düzenlemedir. Bu, federal kurumlar tarafından kayıt sistemlerinde tutulan kişiler hakkında, kişiyi tanımlamak için kullanılan bilgilerin toplanmasını, saklanmasını, kullanılmasını ve dağıtımını düzenleyen Adil Bilgi Uygulama Kurallarını tesis etmektedir. Belirli işlemler için Abbott’a devlet kurumu kayıtlarına erişim izni verilebilir. Bu gibi durumlarda, Abbott, kişiyi tanımlamak için kullanılan bilgilerin korunmasına ilişkin gizlilik eğitimi verildiğinin gösterilmesi dahil olmak üzere, muhtelif yükümlülükleri yerine getirmek zorundadır.Çalışanlar, gizlilik yükümlülükleri olan müşterilerle herhangi bir anlaşma yapmadan önce Hukuk bölümü ile iletişime geçmelidir. |
| [Screen 10](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=17_C_13) [17\_C\_13](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=17_C_13)  | The laws, regulations, and contractual requirements we have just reviewed are often complex and can change rapidly.Abbott has policies and procedures in place to ensure employees comply with these laws and regulations. If you have any questions or want to learn more, contact OEC or a member of the Global Privacy team.For contacts and additional information, click the Resources icon. | Az önce gözden geçirdiğimiz kanunlar, düzenlemeler ve sözleşme gereklilikleri çoğunlukla karmaşıktır ve hızla değişebilir.Abbott, çalışanlarının bu yasa ve düzenlemelere uymasını sağlamak için politika ve prosedürleri uygulamaya koymuştur. Herhangi bir sorunuz varsa veya fazlasını öğrenmek isterseniz, Etik ve Uyum Ofisi veya Global Gizlilik ekibinin bir üyesi ile iletişime geçin.İletişim kişileri ve ek bilgi için Kaynaklar simgesine tıklayın. |
| [Screen 11](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=18_C_14) [18\_C\_14](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=18_C_14)  | Collection* Notice
* Consent

MANAGEMENT* Data Integrity
* Access and Correction

Usage* Disclosure and Use

Disposition* Retention and Disposal

Abbott’s data privacy and protection policies and procedures are organized around a simple set of principles. We call this Privacy by Design.These principles are designed to help employees protect sensitive data at each stage of the data lifecycle. To illustrate, let’s look specifically at personal information.The first stage of the data lifecycle is collection.During this stage, Abbott uses a variety of methods to collect personal information. For example, we may request consumers to provide contact details at an Abbott website, or we may capture personal data generated from one of our devices.In order to protect the privacy rights of the individuals during this stage, we maintain processes to ensure we adhere to the Privacy by Design principles of Notice and Consent.Notice is about letting people know what personal information is being collected and explaining in clear, precise, and unambiguous language how we plan to use that information.For example, when submitting an inquiry at abbott.com, the personal information we collect is used for the sole purpose of responding to the inquiry.Consent is about providing individuals with the opportunity to agree to the collection and use of their personal information.Generally, when we seek consent, we ensure it is:* Freely given. The individual is never coerced or told that consent is a requirement.
* Informed. The individual is given sufficient information to make a reasonable decision to which they are consenting.
* Affirmative. The individual must affirmatively provide consent. We never assign consent, for example, through an individual’s silence, nor do we require the individual to take some action, such as unchecking a box, to opt out of something.
* Revocable. The individual is provided with a clear explanation of how to revoke consent.

For example, a consumer registering with the Abbott Nutrition Similac© Strong Moms© Rewards program can consent to the collection and use of their Personal Information by opting in (e.g., checking a box) to receive additional promotional information.The second stage of the data lifecycle is management.During this stage, information is processed and stored.In order to protect personal information during this stage, we maintain processes that ensure we adhere to the principles of:* Data Integrity, and
* Access and Correction.

Data Integrity is about taking reasonable measures to ensure that the personal information we retain is accurate, complete, and current.One way we do this is by tracking and recording all activities that process personal information. This ensures we can identify the source of the data, the specific purposes for which the data has been processed, and where it is stored.Access and Correction is about providing individuals with reasonable access to their data and the opportunity to exercise their rights in connection with this data.This includes responding to an individual’s request to access, delete, transfer, or amend the stored records of personal information.The third stage of the lifecycle is usage.During this stage, personal information is used to support activities across the organization.In order to protect personal information during this stage, we maintain processes that ensure we adhere to the principle of Disclosure and Use.Disclosure and Use is about controlling who has access to personal information and limiting use to specific purposes.We manage this through access controls and other processes. These controls and processes limit access to individuals in specific job functions as well as limiting use to the specific purposes set out in the notice for which consent was provided.The final stage of the lifecycle is disposition.Disposition refers to what happens to data once it is no longer actively being used. Activities may include deletion, archiving, or retaining for legal hold purposes.In order to protect personal information during this stage, we maintain policies and processes that ensure we adhere to the principle of Retention and Disposal.Retention and Disposal of personal information is about retaining personal information for only the time necessary to achieve the purposes for which it was needed and processed.Once personal information is no longer required in an active production environment, Abbott has put in place processes to either archive or dispose of it in a manner consistent with Abbott’s data management, retention, and disposal requirements. Our retention and disposal requirements are also subject to any legal hold requirements relating to legal matters.For additional information related to retention or disposal requirements, see Abbott’s Global Records and Information Policy (l1-02) or contact Information Governance and Records. Details can be found in the Resources section of this training.For contacts and additional information, click the Resources icon.As we have just seen, our policies and procedures are designed to protect personal information throughout its lifecycle.We do this by adhering to the principles of:* Notice,
* Consent,
* Data Integrity,
* Access and Correction,
* Disclosure and Use, and
* Retention and Disposal.

COLLECTIONNoticeConsentMANAGEMENTData IntegrityAccess and CorrectionUSAGEDisclosure and UseDISPOSITIONRetention and Disposal | Toplama* Bildirim
* Müsaade

YÖNETİM* Veri Bütünlüğü
* Erişim ve Düzeltme

Kullanım* Açıklama ve Kullanım

Elden Çıkarma* Saklama ve İmha

Abbott’ın veri gizliliği ve koruma politikaları ve prosedürleri, yalın bir ilkeler kümesi temel alınarak düzenlenmiştir. Biz buna Tasarım itibarıyla Gizlilik adını veriyoruz.Bu ilkeler, veri yaşam döngüsünün her aşamasında çalışanların hassas verileri korumasına yardımcı olmak için tasarlanmıştır. Örnek olarak, özellikle kişisel bilgilere bir göz atalım.Veri yaşam döngüsünün ilk aşaması, toplama aşamasıdır.Bu aşamada Abbott, kişisel bilgileri toplamak için çeşitli yöntemler kullanır. Mesela, tüketicilerden bir Abbott web sitesine iletişim bilgilerini vermelerini isteyebilir veya cihazlarımızdan biri tarafından üretilen kişisel verileri kayıt altına alabiliriz.Bu aşamada bireylerin gizlilik haklarını korumak için, Bildirim ve Müsaade kapsamındaki Tasarım itibarıyla Gizlilik ilkelerine bağlı kalmamızı sağlayacak süreçler yürütüyoruz.Bildirim, insanlara hangi kişisel bilgilerin toplandığını bildirme ve bu bilgileri nasıl kullanmayı planladığımızı açık, kesin ve belirsizliğe mahal vermeyecek bir dille açıklama ile ilgilidir.Örneğin, abbott.com üzerinden bir talep gönderirken, topladığımız kişisel bilgiler yalnızca bu talebi yanıtlamak amacıyla kullanılır.Müsaade, bireylere kişisel bilgilerinin toplanmasını ve kullanılmasını kabul etme olanağı sağlamakla ilgilidir.Genelde, müsaade istediğimizde, müsaadenin aşağıdaki özellikleri taşıdığından emin oluruz:* Özgürce verilmiş. Bireye müsaadenin bir gereklilik olduğu hakkında asla zorlama uygulanmaz bu veya söylenmez.
* Bilgilendirilmiş. Bireye, müsaade verdikleri konu hakkında akla yatkın bir karar vermeleri için yeterince bilgi verilir.
* Olumlu. Birey müsaadesini olumlu şeklinde vermelidir. Örneğin, bir bireyin sessizliği aracılığıyla müsaade ataması yapamayız veya bireyin bir onay kutusundaki onay işaretini kaldırmak, bir şeyden vazgeçmek gibi eylemler gerçekleştirmesini istemeyiz.
* İptal edilebilir. Bireye, müsaadesinin nasıl iptal edileceğine dair net bir açıklama sağlanır.

Örneğin, Abbott Nutrition Similac © Strong Moms © Rewards programına kayıt olan bir tüketici, ilave promosyon bilgileri almayı seçerek (örn. bir onay kutusunu işaretleyerek) Kişisel Bilgilerinin toplanmasına ve kullanılmasına müsaade edebilir.Veri yaşam döngüsünün ikinci aşaması, yönetim aşamasıdır.Bu aşamada bilgiler işlenir ve saklanır.Bu aşamada kişisel bilgileri korumak için aşağıdaki ilkelere bağlı kalmamızı sağlayan süreçler yürütüyoruz:* Veri Bütünlüğü ve
* Erişim ve Düzeltme.

Veri Bütünlüğü, elimizde bulunan kişisel bilgilerin doğru, eksiksiz ve güncel olmasını sağlamak için makul önlemler almakla ilgilidir.Bunu yapmamızın bir yolu, kişisel bilgileri işleyen tüm aktiviteleri izlemek ve kayıt altına almaktır. Bu, verilerin kaynağını, verilerin spesifik işlenme amaçlarını ve nereye kaydedildiklerini belirleyebilmemizi sağlar.Erişim ve Düzeltme, bireylere kendi verilerine makul düzeyde erişim sunma ve bu verilerle ilgili haklarını kullanma olanağı sağlamayla ilgilidir.Bir bireyin kişisel bilgilerinin saklandığı kayıtlara erişme, bunları silme, aktarma veya değiştirme hususundaki talebine yanıt vermek buna dahildir.Yaşam döngüsünün üçüncü aşaması, kullanım aşamasıdır.Bu aşamada, kişisel bilgiler organizasyon genelindeki faaliyetleri desteklemek için kullanılır.Bu aşamada kişisel bilgileri korumak için, Açıklama ve Kullanım ilkesine bağlı kalmamızı sağlayan süreçler yürütüyoruz.Açıklama ve Kullanım, kişisel bilgilere kimlerin erişebileceğini kontrol etme ve kullanımı belirli amaçlarla sınırlama ile ilgilidir.Bizler, bunu erişim kontrolleri ve diğer süreçler aracılığıyla yönetiyoruz. Bu kontroller ve süreçler; erişimi, belirli görev fonksiyonlarındaki kişilere sınırlandırmanın yanı sıra, kullanımı da, müsaade verilen bildirimle belirtilen özel amaçlarla sınırlandırır.Yaşam döngüsünün son aşaması, elden çıkarma aşamasıdır.Elden çıkarma, artık aktif olarak kullanılmayan verilere ne olduğunu ifade eder. Faaliyetler, silmeyi, arşivlemeyi veya yasal bekletme amaçları için saklamayı içerebilir.Bu aşamada kişisel bilgileri korumak için, Saklama ve İmha ilkesine bağlı kalmamızı sağlayan politikalar ve süreçler yürütüyoruz.Kişisel Bilgilerin Saklanması ve İmha Edilmesi, kişisel bilgileri yalnızca onlara ihtiyaç duyulan amaçlara ve onları işleme amaçlarına ulaşmak için gereken süre boyunca saklama ile ilgilidir.Abbott, aktif bir üretim ortamında kişisel bilgilere artık ihtiyaç kalmadığında, bunların Abbott’ın veri yönetimi, saklama ve imha gerekliliklerine uygun bir şekilde arşivlenmesi veya imha edilmesi için gerekli süreçleri uygulamaya koymuştur. Saklama ve imha gerekliliklerimiz aynı zamanda, hukuki meselelerle ilgili tüm yasal bekletme gerekliliklerine tabidir.Saklama veya imha gereklilikleriyle ilgili ek bilgi almak için, Abbott’ın Global Kayıtlar ve Bilgiler Politikasına (l1-02) bakın veya Bilgi Yönetimi ve Kayıtlar bölümü ile iletişime geçin. Ayrıntılar, bu eğitimin Kaynaklar bölümünde bulunabilir.İletişim kişileri ve ek bilgi için Kaynaklar simgesine tıklayın.Az önce gördüğümüz gibi, politikalarımız ve prosedürlerimiz kişisel bilgileri yaşam döngüsü boyunca korumak üzere tasarlanmıştır.Bunu aşağıdaki ilkelere bağlı kalarak yapıyoruz:* Bildirim,
* Müsaade,
* Veri Bütünlüğü,
* Erişim ve Düzeltme,
* Açıklama ve Kullanım ve
* Saklama ve İmha.

TOPLAMABildirimMüsaadeYÖNETİMVeri BütünlüğüErişim ve DüzeltmeKULLANIMAçıklama ve KullanımELDEN ÇIKARMASaklama ve İmha |
| [Screen 12](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=19_C_15) [19\_C\_15](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=19_C_15)  | Click the arrow to begin your review.ReviewTake a moment to review some of the key concepts covered in this section.Personal Information (PI)PI is any information that can be used to* Contact
* Locate, or
* Identify an individual.

Protected Health Information (PHI)PHI is a particularly sensitive type of personal information used in the healthcare industry.Privacy LawsPrivacy laws differ from one country to the next, but often embrace the same core principles.Abbott’s Privacy by Design PrinciplesAbbott’s data privacy and protection policies and procedures are organized around a set of principles, called Privacy by Design.Notice and ConsentNotice and Consent is about letting people know what PI is being collected and providing them the opportunity to agree to that collection.Data IntegrityData Integrity is about taking reasonable measures to ensure that PI is accurate, complete, and current.Access and CorrectionAccess and Correction is about providing individuals the right to access and correct their data.Disclosure and UseDisclosure and Use is about controlling who has access to PI.Retention and DisposalRetention and Disposal of PI is about retaining personal information for only the time necessary to achieve the purposes for which it was needed and processed.To check your progress, click the Menu buttonGreat job!You have completed section 1 of 4Click the forward arrow to continue learning | İncelemenize başlamak için oka tıklayın.İnceleBu bölümde ele alınan temel kavramların bazılarını incelemek için birkaç dakika ayırın.Kişisel Bilgiler (PI)PI, herhangi bir kişi ile* İletişim kurmak
* Onun yerini belirlemek veya
* Kimliğini belirlemek için kullanılabilecek olan herhangi bir bilgidir.

Korunan Sağlık Bilgileri (PHI)PHI, sağlık hizmetleri sektöründe kullanılan, özellikle hassas bir kişisel bilgi türüdür.Gizlilik YasalarıGizlilik yasaları bir ülkeden diğerine farklılık gösterir ancak genellikle aynı temel ilkeleri benimser.Abbott’ın Tasarım itibarıyla Gizlilik İlkeleriAbbott’ın veri gizliliği ve koruması politikaları ve prosedürleri, Tasarım itibarıyla Gizlilik adı verilen bir dizi ilkeler temel alınarak düzenlenmiştir.Bildirim ve MüsaadeBildirim ve Müsaade, insanların PI toplanmakta olduğunu bilmesini sağlamak ve onlara bu toplamayı kabul etme fırsatı vermek ile ilgilidir.Veri BütünlüğüVeri Bütünlüğü, PI’nin doğru, eksiksiz ve güncel olmasını sağlamak için makul önlemler almakla ilgilidir.Erişim ve DüzeltmeErişim ve Düzeltme, bireylere kendi verilerine erişme ve bu verileri silme hakkı sağlanması ile ilgilidir.Açıklama ve KullanımAçıklama ve Kullanım, PI’ye kimlerin erişimi olduğunu kontrol etmek ile ilgilidir.Saklama ve İmhaPI’yi Saklama ve İmha Etme, kişisel bilgileri yalnızca onlara ihtiyaç duyulan amaçlara ve onları işleme amaçlarına ulaşmak için gereken süre boyunca saklama ile ilgilidir.İlerlemenizi kontrol etmek için Menü düğmesine basınMükemmel!Bölüm 1 / 4’ü tamamladınızÖğrenmeye devam etmek için ileri okuna tıklayın |
| [Screen 13](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=20_C_17) [20\_C\_17](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=20_C_17)  | Another type of sensitive data that we may frequently use is confidential business information.Confidential business information is a broad category. It includes much of the business information we use and come in contact with on a daily basis. Confidential Information is information that is not publicly available that might be of use to Abbott’s competitors or harmful to Abbott if disclosed. | Sıklıkla kullanabileceğimiz bir başka hassas veri türü de gizli ticari bilgidir.Gizli ticari bilgiler kapsamlı bir kategoridir. Buna, her gün kullandığımız ve karşılaştığımız ticari bilgilerinin çoğu dahildir. Gizli Bilgi, Abbott’ın rakiplerinin işine yarayabilecek veya açıklanması durumunda Abbott’a zarar verebilecek olan, herkese açık şekilde mevcut olmayan bilgidir. |
| [Screen 14](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=21_C_18) [21\_C\_18](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=21_C_18)  | Kandice | Marketing Manager Can you give me some examples of confidential business information?Confidential business information can include, but is not limited to: product designs and processes, compositions, organisms, computer software, research and development data, clinical and pharmacological data, patient data, technical data, customer and prospective customer lists, business practices, marketing plans and strategies, financial and operational data, and personnel data.It can also include purchasing information, such as bids for contracts, supplier lists, and costing information. | Kandice | Pazarlama Müdürü Bana bazı gizli ticari bilgi örnekleri verebilir misiniz?Gizli ticari bilgiler arasında sınırlı olmamak kaydıyla şunlar yer alabilir: ürün tasarımları ve süreçleri, bileşimler, organizmalar, bilgisayar yazılımı, araştırma ve geliştirme verileri, klinik ve farmakolojik veri, hasta verisi, teknik veri, müşteri ve potansiyel müşteri listeleri, iş uygulamaları, pazarlama planları ve stratejileri, finansal ve operasyonel veri ve kişisel veri.Bu aynı zamanda, sözleşme teklifleri, tedarikçi listeleri ve maliyet bilgileri gibi satın alma bilgilerini de içerebilir. |
| [Screen 15](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=22_C_19) [22\_C\_19](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=22_C_19)  | Jerry | Sales Representative Are there certain types of confidential business information that are more sensitive than others?Yes. Certain types of confidential business information require greater care than normal because improper disclosure or use of this information can cause serious harm to the company.Examples include:* Trade secrets, manufacturing formulas and processes;
* Clinical and regulatory data, regulatory submissions, or pre-approval information; and
* Financial data that has not been released to the public.
 | Jerry | Satış Temsilcisi Diğerlerinden daha hassas olan belirli türde gizli ticari bilgiler var mı?Evet. Bazı gizli ticari bilgi türleri, normalden daha fazla özen gerektirir; çünkü bu bilgilerin uygunsuz şekilde açıklanması veya kullanılması şirkete ciddi zararlar verebilir.Örnekler arasında şunlar bulunmaktadır:* Ticari sırlar, imalat formülleri ve süreçleri;
* Klinik ve düzenleyici veriler, düzenleyici öneriler veya ön onay bilgileri ve
* Kamuya açıklanmamış olan finansal veriler.
 |
| [Screen 16](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=23_C_20) [23\_C\_20](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=23_C_20)  | As you can see, most of the business information we use in our day-to-day work activities is considered confidential.A good way to confirm whether the business information you are using is confidential is to ask yourself a simple question:Is this information publicly available?If the answer is no, then the information should be considered confidential and appropriate steps must be taken to protect it. | Gördüğünüz üzere, günlük iş faaliyetlerimizde kullandığımız ticari bilgilerinin pek çoğu gizli kabul edilmektedir.Kullandığınız ticari bilgilerinin gizli olup olmadığını teyit etmenin iyi bir yolu, kendinize şu basit soruyu sormaktır:Bu bilgiler kamuya açık mı?Cevap hayır ise, o zaman bilgi gizli kabul edilmeli ve onu korumak için uygun tedbirler alınmalıdır. |
| [Screen 17](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=24_C_20b) [24\_C\_20b](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=24_C_20b)  | It is also important to remember that any confidential business information created as part of your job function at Abbott is Abbott’s property.As a result, you must protect this information and cannot keep it if your Abbott employment ends. | Ayrıca Abbott’taki görev işlevinizin bir parçası olarak geliştirilen herhangi bir gizli ticari bilginin Abbott’ın mülkiyeti olduğunu unutmamak da önemlidir.Bir sonuç olarak, bu bilgileri korumanız gerekir ve Abbott istihdamınız sona ererse bunları elinizde tutamazsınız. |
| [Screen 18](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=25_C_20c) [25\_C\_20c](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=25_C_20c)  | Protecting confidential business information is crucial.Not surprisingly, the improper use or disclosure of this information can result in significant harm to Abbott. | Gizli ticari bilgilerin korunması çok önemlidir.Bekleneceği gibi, bu bilgilerin uygunsuz şekilde kullanılması veya açıklanması Abbott aleyhine önemli bir zararla sonuçlanabilir. |
| [Screen 19](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=26_C_20d) [26\_C\_20d](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=26_C_20d)  | The improper use or disclosure of confidential information can significantly harm Abbott’s relationship with its customers and clients, lead to embarrassing press and media coverage, and result in the loss of competitive advantages for Abbott. It can also result in civil lawsuits and criminal penalties, including against current and former employees.CLICK THE ‘RECENT CASES’ BUTTON FOR MORE INFORMATION. | Gizli bilgilerin uygunsuz şekilde kullanılması veya açıklanması, Abbott’ın müşteriler ve tüketiciler ile olan ilişkisine önemli şekilde zarar verebilir, utandırıcı basın ve medya kapsamına yol açabilir ve Abbott için rekabet avantajlarının kaybı ile sonuçlanabilir. Ayrıca, mevcut ve eski çalışanlara karşı dâhil olmak üzere hukuk davaları ve cezalar ile de sonuçlanabilir.DAHA FAZLA BİLGİ İÇİN ‘SON ZAMANLARDAKİ DAVALAR’ DÜĞMESİNE TIKLAYIN. |
| [Screen 19](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=27_C_20d) [27\_C\_20d](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=27_C_20d)  | RECENT CASESIn recent years, companies have received large jury verdicts and awards against former employees for improperly taking company information. For example, one company received $240 million award against a former employee who improperly disclosed the company’s confidential information to a competitor. Another company received an $854 million jury award against a former employee and his new employer when the former employee misappropriated the company’s confidential information and then used the company’s confidential information on behalf of the new employer.Studies indicate that the theft of confidential information causes losses between $209 and $625 billion to publicly traded companies. | SON ZAMANLARDAKİ DAVALARSon yıllarda şirketler eski çalışanlara karşı şirket bilgilerinin uygunsuz şekilde alınması yüzünden önemli jüri kararları ve lehte hükümler elde etmiştir. Örneğin, bir şirket, şirketin gizli bilgilerini bir rakibe uygunsuz biçimde açıklamış olan eski bir çalışana karşı 240 milyon dolarlık hüküm elde etmiştir. Diğer bir şirket, eski bir çalışanına ve onun yeni işverenine karşı, eski çalışan şirketin gizli bilgilerini zimmetine geçirdiği ve ardından şirketin gizli bilgilerini yeni işveren adına kullandığı için 854 milyon $’lık bir jüri kararı elde etmiştir.Yapılan çalışmalara göre, gizli bilgilerin çalınması, halka açık şirketlerde 209 ile 625 milyar dolar arasında kayıplara yol açmaktadır. |
| [Screen 20](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=28_C_20e) [28\_C\_20e](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=28_C_20e)  | It should come as no surprise that authorities take the theft of confidential information very seriously.For example, under federal criminal statutes, an individual can face up to ten years in prison and a $5 million fine for stealing confidential information. In addition, if a company is found guilty of stealing confidential information, it can be fined $10 million or three times the value of the confidential information.CLICK THE ‘FINES AND PENALTIES’ BUTTON FOR MORE INFORMATION. | Makamların gizli bilgi hırsızlığını ciddiye alması şaşırtıcı gelmemelidir.Örneğin, federal ceza mevzuatı kapsamında, bir birey gizli bilgi çalmaktan dolayı on yıla kadar hapis ve 5 milyon dolar para cezasına çarptırılabilir. Ek olarak, bir şirket gizli bilgi çalmaktan suçlu bulunduğu takdirde 10 milyon dolar veya gizli bilgilerin değerinin üç katı para cezasına çarptırılabilir.DAHA FAZLA BİLGİ İÇİN ‘PARA CEZALARI VE CEZALAR’ DÜĞMESİNE TIKLAYIN. |
| [Screen 20](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=29_C_20e) [29\_C\_20e](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=29_C_20e)  | FINES AND PENALTIESIn recent years, several people and companies have been fined or sentenced to prison for stealing confidential information. For example:* A competitor was fined $60 Million for stealing another company’s confidential information;
* A former IT employee was sentenced to 97 months in prison for stealing confidential information;
* A former salesman was sentenced to 12 months in prison for stealing confidential information;
* A senior executive was sentenced to 24 months in prison for stealing confidential information; and
* A research scientist was sentenced to 18 months in prison for stealing confidential information.
 | PARA CEZALARI VE CEZALARSon yıllarda bazı kişiler ve şirketler gizli bilgi çalmak yüzünden para veya hapis cezası aldı. Örneğin:* Bir rakip başka bir şirketin gizli bilgilerini çalmaktan dolayı 60 milyon dolarlık para cezasına çarptırıldı;
* Eski bir BT çalışanı, gizli bilgi çalmaktan dolayı 97 ay hapis cezasına çarptırıldı;
* Eski bir satış personeli, gizli bilgi çalmaktan dolayı 12 ay hapis cezasına çarptırıldı;
* Kıdemli bir üst düzey yönetici, gizli bilgi çalmaktan dolayı 24 ay hapis cezasına çarptırıldı ve
* Bir araştırma bilim insanı, gizli bilgi çalmaktan dolayı 18 ay hapis cezasına çarptırıldı.
 |
| [Screen 21](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=30_C_21) [30\_C\_21](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=30_C_21)  | Another type of confidential business information that is important to recognize and protect is insider information.Insider information is any non-public, material information that, if publicly disclosed, could reasonably be expected to affect the market value of a company’s securities, or influence investors’ decisions on whether to buy or sell securities. | Anlaşılması ve korunması önemli olan başka bir tür gizli ticari bilgi, yaygın olarak *içeriden bilgi* olarak adlandırılmaktadır.İçeriden bilgi, kamuya açıklandığı takdirde, bir şirketin menkul kıymetlerinin piyasa değerini makul ölçüde etkilemesi veya yatırımcıların menkul kıymet alım satım kararlarını etkilemesi muhtemel kamuya açık olmayan, önemli bilgilerdir. |
| [Screen 22](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=31_C_22) [31\_C\_22](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=31_C_22)  | Examples of insider information include:* News of a potential acquisition,
* A delay in a product launch,
* News of a breach of internal IT systems,
* Unanticipated changes in earnings or dividend rates,
* Proposed tender offers or stock splits,
* Information about major new products,
* Contract awards,
* Expansion plans,
* Significant litigation or regulatory proceedings, etc.
 | İçeriden bilgi örnekleri şunları içerir:* Potansiyel olarak bir şirketi satın almanın haberi,
* Bir ürün lansmanındaki bir gecikme,
* Şirket içi BT sistemlerindeki bir ihlal haberi,
* Kazanç veya temettü oranlarında beklenmeyen değişiklikler,
* Sunulan ihale teklifleri veya hisse senedi bölünmeleri,
* Önemli yeni ürünler hakkındaki bilgiler,
* Kazanılan ihaleler,
* Genişleme planları,
* Önemli hukuk davaları veya mevzuata ilişkin işlemler vb.
 |
| [Screen 23](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=32_C_23) [32\_C\_23](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=32_C_23)  | If you are aware or in possession of insider information, it is illegal to trade in, or recommend others to trade in, Abbott securities.This also applies to the buying and selling of securities of other companies, including those currently doing or expected to do business with Abbott.To learn more about Abbott’s expectations with regard to the use and protection of unpublicized information, review Abbott’s policy on Insider Trading. Details can be found in the Resources section of this training. | İçeriden bilgilerin farkında iseniz veya bu bilgilere sahipseniz, Abbott menkul kıymetlerinin alım satımını yapmak veya başkalarına alım satım yapma tavsiyesi vermek yasa dışıdır.Bu, Abbott ile halihazırda iş yapan veya yapması beklenenler dahil olmak üzere, diğer şirketlerin menkul kıymetlerinin alım satımı için de geçerlidir.Abbott’ın kamuya açıklanmamış bilgilerin kullanımına ve korunmasına ilişkin beklentileri konusunda daha fazla bilgi edinmek için, Abbott’ın İçeriden Bilgi Ticareti hakkındaki politikasını inceleyin. Ayrıntılar, bu eğitimin Kaynaklar bölümünde bulunabilir. |
| [Screen 24](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=33_C_24) [33\_C\_24](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=33_C_24)  | Click the arrow to begin your review.ReviewTake a moment to review some of the key concepts covered in this section.Confidential Business InformationAny business information that is not publicly available should be considered confidential. This includes much of the business information we use in our day-to-day work activities.Improper Use of Confidential Business InformationThe improper use or disclosure of confidential business information can result in significant harm to the Company, our customers and employees.Insider InformationInsider information is any non-public, material information that, if publicly disclosed, could reasonably be expected to affect the market value of a company’s securities, or influence investors’ decisions on whether to buy or sell securities.To check your progress, click the Menu buttonGreat job!You have completed section 2 of 4Click the forward arrow to continue learning | İncelemenize başlamak için oka tıklayın.İnceleBu bölümde ele alınan temel kavramların bazılarını incelemek için birkaç dakika ayırın.Gizli Ticari BilgilerHerkese açık şekilde mevcut olmayan herhangi bir şirket bilgisi gizli olarak kabul edilmelidir. Bunlar, günlük iş faaliyetlerimizde kullandığımız ticari bilgilerinin çoğunu içerir.Gizli Ticari Bilgilerin Uygunsuz KullanımıGizli ticari bilgilerin uygunsuz şekilde kullanılması veya açıklanması, Şirket, müşterilerimiz ve çalışanlarımız için önemli bir zararla sonuçlanabilir.İçeriden Bilgiİçeriden bilgi, kamuya açıklandığı takdirde, bir şirketin menkul kıymetlerinin piyasa değerini makul ölçüde etkilemesi veya yatırımcıların menkul kıymet alım satım kararlarını etkilemesi muhtemel kamuya açık olmayan, önemli bilgilerdir.İlerlemenizi kontrol etmek için Menü düğmesine basınMükemmel!Bölüm 2 / 4’ü tamamladınızÖğrenmeye devam etmek için ileri okuna tıklayın |
| [Screen 25](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=34_C_25) [34\_C\_25](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=34_C_25)  | Now that you have a good understanding of the different kinds of data you are likely to encounter during your workday, here is what you can do to help protect it. | Artık mesai gününüz boyunca karşılaşabileceğiniz farklı türdeki verileri iyice anladığınıza göre, bunları korumaya yardımcı olmak için yapabileceklerinizi burada bulabilirsiniz. |
| [Screen 26](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=35_C_26) [35\_C\_26](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=35_C_26)  | Before accessing any sensitive data, make sure your role and responsibilities require you to access the data.If you have a question about whether you should access the data, especially with respect to personal information, contact your manager, the OEC or a member of the Global Privacy team.CLICK THE ‘DID YOU KNOW’ BUTTON FOR MORE INFORMATION. | Herhangi bir hassas veriye erişmeden önce, görevinizin ve sorumluluklarınızın verilere erişmenizi gerektirdiğinden emin olun.Özellikle kişisel bilgilerle ilgili olarak verilere erişmeniz gerekip gerekmediğine ilişkin bir sorunuz varsa yöneticiniz, Etik ve Uyum Ofisi veya Global Gizlilik ekibinin bir üyesi ile görüşün.DAHA FAZLA BİLGİ İÇİN ‘BİLİYOR MUYDUNUZ’ DÜĞMESİNE TIKLAYIN. |
| [Screen 26](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=36_C_26) [36\_C\_26](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=36_C_26)  | DID YOU KNOWAbbott engages in various forms of lawful monitoring to reduce the risk of improper data usage.This include monitoring the downloading of data or the sending of data to non-Abbott email addresses. | BİLİYOR MUYDUNUZAbbott, uygunsuz veri kullanımı riskini azaltmak için çeşitli yasal izleme şekilleri kullanmaktadır.Bunlar arasında veri indirmenin veya Abbott dışı e-posta adreslerine veri göndermenin izlenmesi bulunmaktadır. |
| [Screen 27](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=37_C_27) [37\_C\_27](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=37_C_27)  | If you have permission to access sensitive data, only use it for the specific purpose for which you have been granted access.In the case of personal information, only use the data according to the consent given or notice provided. | Hassas verilere erişim izniniz varsa, bunu yalnızca size erişim izni verilen spesifik amaç dahilinde kullanın.Kişisel bilgiler söz konusu olduğunda, verileri yalnızca verilen müsaadeye veya bildirime uygun şekilde kullanın. |
| [Screen 28](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=38_C_30) [38\_C\_30](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=38_C_30)  | Before sharing sensitive data, make sure the person you plan to share with has proper authorization.If you have a question about whether you should access the data, especially with respect to personal information, talk to your manager or a member of Abbott’s Privacy team. | Hassas verileri paylaşmadan önce, paylaşmayı planladığınız kişinin uygun yetkiye sahip olduğundan emin olun.Özellikle kişisel bilgilerle ilgili olarak, verilere erişmeniz gerekip gerekmediğine ilişkin bir sorunuz varsa amiriniz veya bir Abbott Gizlilik ekibi üyesi ile görüşün. |
| [Screen 29](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=39_C_31) [39\_C\_31](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=39_C_31)  | Requests from Your Own CountryIf an Abbott employee located in your same country requests sensitive data, always:* Confirm the identity of the person making the request;
* Confirm the person’s need to access the information;
* Check to make sure the person is authorized to receive the information;
* Verify that the information can be used for the requested purpose; and
* Share only the amount of information required to meet the need, not more.

If in doubt, contact OEC or Global Privacy prior to sharing sensitive data. | Kendi Ülkenizden Gelen İsteklerSizinle aynı ülkede bulunan bir Abbott çalışanı sizden hassas veri talep ederse, her zaman:* İstekte bulunan kişinin kimliğini teyit edin;
* Kişinin bilgilere erişim gerekçesini teyit edin;
* Kişinin, bilgileri elde etme yetkisine sahip olup olmadığını kontrol edin;
* Bilgilerin talep edilen amaç için kullanılabileceğini teyit edin ve
* Fazlasını değil, yalnızca ihtiyacı karşılamak için gereken miktarda bilgiyi paylaşın.

Şüpheniz varsa, hassas verileri paylaşmadan önce Etik ve Tam Uyum Ofisi veya Global Gizlilik ile iletişime geçin. |
| [Screen 30](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=40_C_32) [40\_C\_32](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=40_C_32)  | Requests from Other CountriesMany countries and regions have laws designed to protect the rights of their citizens, and place restrictions on the transference of personal information across national borders.If you receive a request for information containing sensitive data from a colleague in a different country than your own, check your division or function’s data privacy policies, or consult OEC or Global Privacy before proceeding. Then, follow the same steps you would if responding to a request from a colleague in your own country. | Diğer Ülkelerden Gelen İsteklerBirçok ülke ve bölge, vatandaşlarının haklarını korumak için tasarlanmış yasalar uygulamakta ve kişisel bilgilerin ulusal sınırların ötesine aktarılmasına kısıtlamalar getirmektedir.Kendinizinkinden farklı bir ülkedeki bir çalışma arkadaşınızdan hassas veriler içeren bir bilgi talebi alırsanız, devam etmeden önce bölümünüzün veya fonksiyonunuzun veri gizliliği politikalarını kontrol edin veya Etik ve Tam Uyum Ofisine veya Global Gizlilik bölümüne danışın. Sonra, kendi ülkenizde yerleşik bir iş arkadaşınızdan gelen isteğe cevap verirken izlediğiniz adımları izleyin. |
| [Screen 31](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=41_C_33) [41\_C\_33](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=41_C_33)  | Requests from Third PartiesIf the request for sensitive data is from a third party, ensure there is a valid and appropriate contractual agreement in place. If you are unsure, contact OEC, Global Privacy, or Legal prior to sharing. | Üçüncü Taraflardan Gelen İsteklerHassas veri talebi üçüncü bir taraftan geliyorsa, geçerli ve uygun bir sözleşmenin yürürlükte olduğundan emin olun. Emin değilseniz, paylaşmadan önce Etik ve Tam Uyum Ofisi veya Global Gizlilik ve Hukuk bölümü ile iletişime geçin. |
| [Screen 32](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=42_C_35) [42\_C\_35](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=42_C_35)  | Always archive or dispose of sensitive data in a manner consistent with Abbott’s data management, retention, and disposal requirements. | Hassas verileri, daima Abbott’ın veri yönetimi, saklama ve imha gerekliliklerine uygun bir şekilde arşivleyin veya imha edin. |
| [Screen 33](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=43_C_36) [43\_C\_36](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=43_C_36)  | If you receive a legal hold order, you are prohibited from discarding, destroying, or deleting any information covered by the hold.If you have questions related to legal hold orders or retention and disposal, contact the attorney/paralegal listed in the Legal Hold notification, or call the Litigation Department at (224) 667-5701. | Bir yasal bekletme emri alırsanız, bekletme kapsamındaki herhangi bir bilgiyi atmanız, yok etmeniz veya silmeniz yasaktır.Yasal bekletme emirleri veya saklama ve imha ile ilgili herhangi bir sorunuz varsa, Yasal Bekletme bildiriminde belirtilen avukat/yardımcı avukat ile iletişime geçin veya (224) 667-5701 numaradan Yasal Anlaşmazlıklar Bölümünü arayın. |
| [Screen 34](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=44_C_37) [44\_C\_37](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=44_C_37)  | Always take special care with sensitive data when someone leaves Abbott.Managers must ensure the departing employee is terminated in the appropriate system (e.g., Workday for Employees or Fieldglass for Contingent Workers) as soon as they are notified the employee is leaving. This will ensure access to Abbott data, physical access to buildings, and final pay will be properly managed. | Abbott’tan biri ayrıldığında hassas verilere daima özel itina gösterin.Yöneticiler, bir çalışanın işten ayrılmakta olduğu kendilerine bildirilir bildirilmez, işten ayrılan çalışanın ilgili sistemde (örneğin, Çalışanlar için Workday veya Taşeron İşçiler için Fieldglass) feshedilmesini sağlamak zorundadır. Bu, Abbott verilerine erişimin, binalara fiziksel erişimin ve nihai ödemenin düzgün bir şekilde yönetilmesini sağlayacaktır. |
| [Screen 35](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=45_C_37b) [45\_C\_37b](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=45_C_37b)  | Ensure no sensitive data leaves with the departing employee. Transition all files to the Abbott employee who will be assuming the departing person’s role or responsibilities.Remind the departing employee of the obligation not to keep or disclose sensitive information. Employees may not take their work product or any other Abbott property (e.g. mobile devices) with them when they leave Abbott. If you have questions about your local termination process, contact Human Resources. | İşten ayrılan çalışan ile birlikte hiçbir hassas verinin gitmemesini sağlayın. Tüm dosyaları, ayrılan kişinin rolünü veya sorumluluklarını üstlenecek olan Abbott çalışanına aktarın.İşten ayrılan çalışana hassas verileri elde tutmama veya açıklamama yükümlülüğünü hatırlatın. Çalışanlar Abbott’tan ayrılırken kendi çalışma ürünlerini veya herhangi bir başka Abbott malını (örneğin mobil cihazları) beraberlerinde götüremez. Yerel fesih süreciniz ile ilgili sorularınız olursa İnsan Kaynakları ile iletişime geçin. |
| [Screen 36](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=46_C_38) [46\_C\_38](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=46_C_38)  | Inadvertent disclosures of PHI can happen at any time.For example, you may overhear a nurse discussing details of a patient’s health status or you may accidentally be copied on an email containing details of a patient’s record. | Herhangi bir zamanda istenmeden PHI açıklamaları yer alabilir.Örneğin, bir hemşirenin bir hastanın sağlık durumu detaylarına ilişkin konuşmasına kulak misafiri olabilir veya bir hasta kaydının ayrıntılarını içeren bir e-postaya yanlışlıkla eklenebilirsiniz. |
| [Screen 37](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=47_C_38a) [47\_C\_38a](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=47_C_38a)  | In response to any inadvertent or improper disclosure of a patient’s protected health information (PHI), you should immediately report the incident to OEC or a member of the Global Privacy team. | Bir hastanın korunan sağlık bilgilerinin (PHI) yanlışlıkla veya uygunsuz şekilde açıklanması karşısında vakayı hemen Etik ve Tam Uyum Ofisine veya Global Gizlilik ekibinin bir üyesine bildirmeniz gerekir. |
| [Screen 38](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=48_C_38b) [48\_C\_38b](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=48_C_38b)  | If you become aware of the improper or inadvertent disclosure of Confidential Business Information, you should immediately report the disclosure to both:* Your direct supervisor, and
* OEC or a member of the Global Privacy team.

Your immediate reporting of the disclosure will help Abbott immediately retrieve the information, prevent additional improper or misuse of the information and if appropriate, assist the company with pursuing civil or criminal action. | Gizli Ticari Bilgilerin uygunsuz biçimde veya yanlışlıkla açıklandığını öğrenirseniz, bu açıklamayı şunların her ikisine de bildirmeniz gerekir:* Doğrudan amiriniz ve
* Etik ve Tam Uyum Ofisi veya Global Gizlilik ekibinin bir üyesi.

İfşayı hemen raporlamanız, Abbott’ın bilgiyi geri almasına, bilginin ek olarak uygunsuz veya kötü amaçlı kullanımını önlemesine ve uygunsa, şirketin hukuki ve cezai işlemi başlatmasına yardımcı olacaktır. |
| [Screen 39](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=49_C_38c) [49\_C\_38c](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=49_C_38c)  | You should never disclose Abbott sensitive data to anyone not authorized to receive the sensitive data.Similarly, you should only use Abbott sensitive data on behalf of Abbott and while performing your Abbott business function.If you improperly disclose sensitive data, you may face disciplinary action, up to and including termination of employment. | Abbott hassas verilerini, hassas veriyi almak için yetkilendirilmiş olmayan bir kişiye asla ifşa etmemelisiniz.Benzer şekilde, Abbott hassas verisini sadece Abbott adına ve Abbott iş fonksiyonunuzu yerine getirirken kullanmalısınız.Hassas bilgileri uygunsuz şekilde açıklarsanız istidamın feshedilmesine varacak şekilde disiplin işlemi ile karşı karşıya kalabilirsiniz. |
| [Screen 40](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=50_C_38d) [50\_C\_38d](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=50_C_38d)  | You are not permitted, both during and after your Abbott employment, to share Abbott data with any Abbott competitor. | Hem Abbott’taki istihdamınız sırasında hem sonrasında Abbott verilerini herhangi bir Abbott rakibi ile paylaşmanıza da izin yoktur. |
| [Screen 41](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=51_C_38e) [51\_C\_38e](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=51_C_38e)  | Failure to return sensitive data to Abbott, transmitting sensitive data to an unapproved device, storage, account or server, or providing sensitive data to any person or entity not authorized to possess the information can lead to Abbott pursuing legal action against you.CLICK THE ‘LEGAL ACTION’ BUTTON FOR MORE INFORMATION. | Hassas verileri Abbott’a iade etmemek, hassas verileri onaysız bir cihaza, depoya, hesaba veya sunucuya iletmek veya hassas verileri, bu bilgileri bulundurma yetkisi olmayan herhangi bir kişiye veya tüzel kişiliğe sağlamak Abbott’ın size karşı yasal işlem başlatmasına yol açabilir.DAHA FAZLA BİLGİ İÇİN ‘YASAL İŞLEM’ DÜĞMESİNE TIKLAYIN. |
| [Screen 41](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=52_C_38e) [52\_C\_38e](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=52_C_38e)  | LEGAL ACTIONLegal action could include Abbott filing a civil lawsuit against you that would:* Prevent you from working for a new employer until Abbott sensitive data has been returned and protected;
* Require you to turn over all electronic devices to Abbott for review and inspection;
* Cause you to pay monetary damages for illegally retaining and/or using Abbott sensitive data, and violating the duties and obligations you owe Abbott under your Abbott Employment Agreement; and
* Obligate you to pay the legal fees Abbott incurs as a result of filing a lawsuit to protect its sensitive data.

If necessary, Abbott will also work with local, state and federal authorities to protect and retain Abbott sensitive data. In this scenario, you could also face criminal penalties. | YASAL İŞLEMYasal işlem, Abbott’ın aşağıdaki amaçlarla size karşı bir hukuki davanın açılmasını içerebilir:* Abbott hassas verileri iade edilinceye ve korununcaya kadar sizin yeni bir işveren için çalışmanızı önlemek;
* Tüm elektronik cihazları incelemek ve muayene etmek için Abbott’a iade etmenizi zorunlu tutmak;
* Yasadışı olarak Abbott hassas verilerini bulundurmanıza ve/veya kullanmanıza ve Abbott İstihdam Anlaşmanız kapsamında Abbot’ta borçlu olduğunuz yükümlülükleri ihlal etmenize ilişkin parasal tazminat ödemenizi sağlamak ve
* Abbott’a, kendi hassas verilerini korumak için dava açmanın sonucu olarak yüklendiği yasal ücretleri ödemenizi zorunlu tutmak.

Gerekirse, Abbott Abbott hassas verilerini korumak ve elde tutmak için yerel, eyalet ve federal makamlar ile birlikte de çalışacaktır. Bu senaryoda, cezai yaptırımlarla da karşılaşabilirsiniz. |
| [Screen 42](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=53_C_43) [53\_C\_43](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=53_C_43)  | Any event involving a potential compromise of information security, including a lost or stolen mobile device, should be reported immediately to your local Global Service Desk.If you have any concerns about a potential violation or want to report a potential privacy incident, contact Global Privacy. | Kayıp veya çalınmış mobil cihazlar dahil olmak üzere, bilgi güvenliğinin potansiyel ihlali ile ilgili her türlü olay derhal yerel Global Servis Masasına bildirilmelidir.Potansiyel bir ihlal hakkında herhangi bir endişeniz varsa veya muhtemel bir gizlilik ihlali vakasını bildirmek istiyorsanız Global Gizlilik ile iletişime geçin. |
| [Screen 43](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=54_C_44) [54\_C\_44](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=54_C_44)  | Click the arrow to begin your review.ReviewTake a moment to review some of the key concepts covered in this section.Accessing and Using Sensitive DataOnly access and use sensitive data for the specific purpose for which you have been granted access.Sharing Sensitive DataBefore sharing sensitive data:* Confirm the identity of the requestor;
* Confirm their need to access the information;
* Verify the information can be used for the purpose(s) requested; and
* Share only the amount required to meet the need.

Retaining and Disposing of Sensitive DataAlways archive or dispose of sensitive data in a manner consistent with Abbott’s data management, retention, and disposal requirements.Responding to Inadvertent Disclosure of PHIIn response to any inadvertent or improper disclosure of a patient’s PHI, immediately report the disclosure to OEC or a member of the Global Privacy team.Reporting a Privacy IncidentContact the Global Privacy team to report a potential privacy incident.To check your progress, click the Menu buttonGreat job!You have completed section 3 of 4Click the forward arrow to continue learning | İncelemenize başlamak için oka tıklayın.İnceleBu bölümde ele alınan temel kavramların bazılarını incelemek için birkaç dakika ayırın.Hassas Verilere Erişim ve KullanımHassas verilere yalnızca size erişim izni verilen söz konusu amaç için erişin ve onları kullanın.Hassas Verilerin PaylaşılmasıHassas verileri paylaşmadan önce:* Talep sahibinin kimliğini teyit edin;
* Kendisinin bilgilere erişme ihtiyacını teyit edin;
* Bilgilerin talep edilen amaç(lar) için kullanılabileceğini teyit edin ve
* Yalnızca ihtiyacı karşılamak için gereken miktarı paylaşın.

Hassas Verilerin Saklanması ve İmhasıHassas verileri, daima Abbott’ın veri yönetimi, saklama ve imha gerekliliklerine uygun bir şekilde arşivleyin veya imha edin.PHI’nin Yanlışlıkla İfşasına MüdahaleBir hastanın PHI’sinin yanlışlıkla veya uygunsuz şekilde açıklanması karşısında açıklamayı hemen Etik ve Tam Uyum Ofisine veya Global Gizlilik ekibinin bir üyesine bildirin.Bir Gizlilik Vakasının BildirilmesiPotansiyel bir gizlilik vakasını bildirmek için Global Gizlilik ekibi ile iletişime geçin.İlerlemenizi kontrol etmek için Menü düğmesine basınMükemmel!Bölüm 3 / 4’ü tamamladınızÖğrenmeye devam etmek için ileri okuna tıklayın |
| [Screen 44](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=55_C_45) [55\_C\_45](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=55_C_45)  | Where to Get HelpOffice of Ethics and Compliance (OEC)Global Privacy – Contact Global Privacy via email at privacy@abbott.com. You can find additional contact details and important information about privacy on the Global Privacy Portal [here](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/GBLPRIV/Pages/Main/default.aspx) on Abbott World.OEC Contacts – You are encouraged to contact the OEC at any time with any ethics and compliance questions, or to discuss concerns about possible violations of our written standards, laws, or regulations.* Visit the [Contact OEC](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/About/Pages/Contacts.aspx) page on the [OEC website](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/Pages/Home.aspx) on Abbott World or OEC@abbott.com.

ENTERPRISE CYBERSECURITYVisit the Enterprise Cybersecurity site [here](https://abbott.sharepoint.com/sites/abbottworld/InformationTechnology/ISRM/Pages/default.aspx) on Abbott World.Visit the [Simply Digital](https://abbott.sharepoint.com/teams/GLB-BTS-ssdw/SitePages/Home.aspx) site to learn about secure ways to share information.Legal DivisionContact the [Legal Division](https://abbott.sharepoint.com/sites/abbottworld/Legal/Pages/Home.aspx?icid=AW_MN_ORG_Legal) with questions or concerns about third-party contractual obligations regarding privacy and data protection.Contact the Information Governance team at information.governance@abbott.com with questions or concerns regarding retention requirements or for guidance on acceptable use of technology solutions.REFERENCE POLICIES:* Click [here](http://abbottmfiles.oneabbott.com/#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?limit=499&00_p100=107&01_p1170*=GLB-CONF-INFO&06_p39=138_p2C131&resultsFromEachRepository=true&includeUnmanaged=true) to review the Confidential Information Policy
* Click [here](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/training/Pages/Insider_Trading.aspx) to review Abbott’s policy on Insider Trading
* Click [here](http://abbottmfiles.oneabbott.com/Default.aspx#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?00_p1170=GLB-TECHNOLOGY-USE&01_p100=107&02_p39=131&showopendialog=0) to review the Acceptable Technology Use Policy.
* Click [here](http://abbottmfiles.oneabbott.com/Default.aspx#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?00_p1170=I1-02&01_p100=107&02_p39=131&showopendialog=0) to review the Records and Information Policy on M-Files.

OEC Policies and ProceduresFor our company’s global and country-specific OEC policies and procedures:* Abbott employees should visit [iComply](https://icomply.abbott.com/Default.aspx).

Human Resources Service Center* Click [here](http://webstorage.abbott.com/hr/126_HR_Service_Center_Contact_List_English.pdf) for a list of HR support contact numbers.

Course ResourcesTranscriptClick [here](file:///D%3A/development/AbbottProtectSensitiveInfo/courses/EN-US/translation/reference/Transcript.pdf) for a full transcript of the course. | Nereden Yardım Almalı?Etik ve Uyum Ofisi (OEC)Global Güvenlik – Global Güvenlik ile privacy@abbott.com adresinden e-posta ile iletişime geçin. İlave iletişim bilgilerini ve gizlilikle ilgili önemli bilgileri Abbott World sitesinde [buradan](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/GBLPRIV/Pages/Main/default.aspx) Global Gizlilik Portalına girerek edinebilirsiniz.Etik ve Tam Uyum (OEC) Temsilcileri – Etik ve Tam Uyum ile herhangi bir etik ve uyum sorusu hakkında her zaman iletişime geçmeniz veya yazılı standartlar, kanunlar ya da düzenlemelere ait olası ihlaller hakkındaki endişeleri görüşmeniz için teşvik edilmektesiniz.* Abbott World üzerinde [OEC web sitesindeki](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/Pages/Home.aspx) [OEC İletişim](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/About/Pages/Contacts.aspx) sayfasını ziyaret edin veya OEC@abbott.com adresine yazın.

KURUMSAL SİBER GÜVENLİKAbbott World’deki Kurumsal Siber Güvenlik sitesini [buradan](https://abbott.sharepoint.com/sites/abbottworld/InformationTechnology/ISRM/Pages/default.aspx) ziyaret edin.Bilgi paylaşmanın güvenli yolları hakkında bilgi almak için [Basitçe Dijital](https://abbott.sharepoint.com/teams/GLB-BTS-ssdw/SitePages/Home.aspx) sitesini ziyaret edin.Hukuk BölümüGizlilik ve veri koruma ile ilgili üçüncü taraf sözleşme yükümlülükleri konusundaki sorunlarınız veya endişeleriniz için [Hukuk Bölümü](https://abbott.sharepoint.com/sites/abbottworld/Legal/Pages/Home.aspx?icid=AW_MN_ORG_Legal) ile iletişime geçin.Saklama gereklilikleriyle ilgili soru veya sorunlarınız için veya teknoloji çözümlerinin kabul edilebilir kullanımına ilişkin rehberlik için information.governance@abbott.com adresinden Bilgi Yönetimi ekibiyle iletişime geçin.REFERANS POLİTİKALAR:* Gizli Bilgi Politikasını gözden geçirmek için [buraya](http://abbottmfiles.oneabbott.com/#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?limit=499&00_p100=107&01_p1170*=GLB-CONF-INFO&06_p39=138_p2C131&resultsFromEachRepository=true&includeUnmanaged=true) tıklayın
* Abbott’ın İçeriden Bilgi Ticareti hakkındaki politikasın gözden geçirmek için [buraya](https://abbott.sharepoint.com/sites/abbottworld/EthicsCompliance/training/Pages/Insider_Trading.aspx) tıklayın
* Kabul Edilebilir Teknoloji Kullanım Politikasını gözden geçirmek için [buraya](http://abbottmfiles.oneabbott.com/Default.aspx#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?00_p1170=GLB-TECHNOLOGY-USE&01_p100=107&02_p39=131&showopendialog=0) tıklayın.
* M-Files üzerinde Kayıtlar ve Bilgi Politikasını gözden geçirmek için [buraya](http://abbottmfiles.oneabbott.com/Default.aspx#3E4088E6-D40A-4DA2-90B9-76B55D51A390/views/_tempsearch?00_p1170=I1-02&01_p100=107&02_p39=131&showopendialog=0) tıklayın.

Etik ve Tam Uyum Politikaları ve ProsedürleriŞirketimizin küresel ve ülkeye özgü Etik ve Uyum Ofisi politikaları ve prosedürleri için:* Abbott çalışanları [iComply](https://icomply.abbott.com/Default.aspx) sayfasını ziyaret etmelidir.

İnsan Kaynakları Hizmet Merkezi* İK destek iletişim numaralarının listesi için [buraya](http://webstorage.abbott.com/hr/126_HR_Service_Center_Contact_List_English.pdf) tıklayın.

Kurs KaynaklarıTranskriptKursun tam bir transkripti için [buraya](file:///D%3A/development/AbbottProtectSensitiveInfo/courses/EN-US/translation/reference/Transcript.pdf) tıklayın. |
| [Screen 45](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=56_C_47) [56\_C\_47](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=56_C_47)  | The Knowledge Check consists of 10 questions. You must score 80% or higher to successfully complete this course.When you are ready, click the Knowledge Check button. | Bilgi Kontrolü 10 soruyu içermektedir. Bu kursu başarıyla tamamlamak için %80 veya daha yüksek puan almalısınız.Hazır olduğunuzda, **Bilgi Kontrolü** düğmesine tıklayın. |
| Screen 46Question 1: Scenario57\_C\_48 | Assuming you have worked for Abbott for several years and have recently accepted an offer to work for another company, which of the following would you be legally allowed to take with you when you leave? | Abbott’ta birkaç yıl çalıştığınızı ve kısa süre önce başka bir şirkette çalışmak için bir teklifi kabul ettiğini varsayarak, ayrılırken aşağıdakilerin hangilerini yanınıza almanıza yasal bakımdan izin olacaktır? |
| Screen 46Question 1: Options58\_C\_48 | [1] Personal Patient Information from clinical studies[2] Abbott customers lists and presentation information that you created while working for Abbott[3] Sales projections and financial data for your Abbott Division or Business Unit[4] Personal photos and mementos | [1] Klinik çalışmalardan Kişisel Hasta Bilgileri[2] Abbott için çalışırken oluşturduğunuz Abbott müşteri listeleri ve sunum bilgileri[3] Abbott Bölümünüz ve İş Biriminiz için satış projeksiyonları ve mali veriler[4] Kişisel fotoğraflar ve hatıra eşyaları |
| Screen 46Question 1: Feedback59\_C\_48 | The correct answer is 4. Personal information, confidential business information, and Protected Health Information are all considered sensitive data that you cannot take with you or use after leaving Abbott. Additionally, all Abbott electronic devices and other Abbott property must be returned prior to leaving.For more information, see  Section 3.4, Responding to Improper Disclosures.  | Doğru yanıt 4’tür. Kişisel Bilgiler, gizli ticari bilgiler ve Korunan sağlık bilgileri hep, beraberinizde götüremeyeceğiniz veya Abbott’tan ayrıldıktan sonra kullanamayacağınız hassas veriler olarak kabul edilmektedir. Ek olarak, Abbott elektronik cihazları ve diğer Abbott malları ayrılmadan önce iade edilmek zorundadır.Daha fazla bilgi için bkz.  Bölüm 3.4, Uygunsuz İfşalara Müdahale.  |
| Screen 46Question 2: Scenario60\_C\_48 | A Marketing Manager is working on a new product launch and must create a consent form for potential customers. The form will allow for the collection and use of personal information. To align with Abbott’s practices for consent, which of the following must be true for the consent form?Check all that apply. | Bir Pazarlama Müdürü yeni bir ürün lansmanı üzerinde çalışmaktadır ve potansiyel müşteriler için bir müsaade formu oluşturmak zorundadır. Bu form kişisel bilgi toplanmasına ve kullanılmasına izin verecektir. Abbott’ın müsaade uygulamalarına uygun olması için, müsaade formu için aşağıdakilerin hangilerinin doğru olması gerekir?Geçerli olan tüm seçenekleri işaretleyin. |
| Screen 46Question 2: Options61\_C\_48 | [1] The form must not pressure customers into giving their consent.[2] The form must provide customers with all the information about how their personal information will be used.[3] The form must require customers to actively agree to the collection and use of their personal information.[4] The form must not allow customers to withdraw their consent once they have given it. | [1] Form, müşterilere müsaade vermeleri için baskı yapmamalıdır.[2] Form, müşterilere, kişisel bilgilerinin nasıl kullanılacağı hakkındaki tüm bilgileri vermelidir.[3] Form, müşterilerin, kişisel bilgilerinin toplanmasını ve kullanılmasını aktif şekilde kabul etmesini istemelidir.[4] Form, müşterilerin bir kez müsaade verdikten sonra onu geri çekmesine olanak sağlamamalıdır. |
| Screen 46Question 2: Feedback62\_C\_48 | Abbott's practices for consent require that the form:* Be clear and concise.
* Not pressure people into giving their consent.
* Provide all information about how personal information will be used.
* Require people to actively agree to the collection and use of their personal information.
* Allow withdrawal of consent if desired.

For more information, see  Section 1.3, Abbott’s Privacy by Design Principles.  | Abbott’ın müsaade uygulamaları formun şu şekilde olmasını gerektirir:* Anlaşılır ve öz olmak.
* İnsanlara müsaade vermeleri için baskı yapmamak.
* Kişisel bilgilerin nasıl kullanılacağı hakkındaki tüm bilgileri sağlamak.
* İnsanların kişisel bilgilerinin toplanmasını ve kullanılmasını aktif şekilde kabul etmesini istemek.
* İstendiği takdirde müsaadenin geri çekilmesine olanak sağlamak.

Daha fazla bilgi için bkz.  Bölüm 1.3, Abbott’ın Tasarım itibarıyla Gizlilik İlkeleri.  |
| Screen 46Question 3: Scenario63\_C\_48 | Disclosure and Use of sensitive data such as personal information is managed at Abbott through: | Kişisel bilgiler gibi hassas verilerin Açıklanması ve Kullanılması Abbott’ta aşağıdaki şekilde yönetilir: |
| Screen 46Question 3: Options64\_C\_48 | [1] De-identification of all data.[2] Access controls.[3] Both 1 and 2. | [1] Tüm verilerin kimliksizleştirilmesi.[2] Erişim kontrolleri.[3] Hem 1 hem 2. |
| Screen 46Question 3: Feedback65\_C\_48 | Disclosure and Use of personal information are managed through access controls and other processes that limit access and use to individuals in specific job functions and for the specific purposes set out in the notice for which consent was given.For more information, see  Section 1.3, Abbott’s Privacy by Design Principles.  | Kişisel bilgilerin Açıklanması ve Kullanılması, bireylerin erişimini ve kullanımını belirli görev fonksiyonlarıyla ve müsaadenin verildiği bildirimde belirtilen özel amaçlarla sınırlayan erişim kontrolleri ve diğer süreçler aracılığıyla yönetilir.Daha fazla bilgi için bkz.  Bölüm 1.3, Abbott’ın Tasarım itibarıyla Gizlilik İlkeleri.  |
| Screen 46Question 4: Scenario66\_C\_48 | Which of the following is true in relation to the retention and disposal of personal information?Check all that apply. | Kişisel bilgilerin saklanması ve imha edilmesi bakımından aşağıdakilerin hangisi doğrudur?Geçerli olan tüm seçenekleri işaretleyin. |
| Screen 46Question 4: Options67\_C\_48 | [1] Personal information is only retained for the time necessary to achieve the purposes for which it was collected and processed.[2] Once data is no longer required in an active production environment, it should always be disposed of.[3] Retention and disposal of personal information is subject to any holds relating to legal matters. | [1] Kişisel bilgiler, yalnızca toplanma ve işlenme amaçlara ulaşmak için gereken süre boyunca saklanır.[2] Veriler, aktif bir üretim ortamında onlara artık ihtiyaç kalmadığında daima imha edilmelidir.[3] Kişisel Bilgilerin saklanması ve imha edilmesi, yasal konularla ilgili tüm bekletmelere tabidir. |
| Screen 46Question 4: Feedback68\_C\_48 | Generally, Abbott should only retain personal information for the time necessary to achieve the purposes for which it was collected and processed. Once data is no longer required in an active production environment, it should be either archived or disposed of, in a manner consistent with Abbott’s data management, retention, and disposal requirements. Retention and disposal requirements are also subject to any holds relating to legal matters.For more information about the correct answer, Section 1.3, Abbott’s Privacy by Design Principles. | Genel olarak Abbott, kişisel bilgileri yalnızca toplanma ve işlenme amaçlarına ulaşmak için gereken süre boyunca saklamalıdır. Aktif bir üretim ortamında artık verilere ihtiyaç kalmadığında, veriler Abbott’ın veri yönetimi, saklama ve imha gerekliliklerine uygun bir şekilde arşivlenmeli veya imha edilmelidir. Saklama ve imha gereklilikleri, hukuki konularla ilgili tüm bekletmelere de tabidir.Doğru yanıt hakkında daha fazla bilgi için Bölüm 1.3, Abbott’ın Tasarım itibarıyla Gizlilik İlkeleri. |
| Screen 46Question 5: Scenario69\_C\_48 | An Engineer is working on developing a new product. Which of the following would be considered confidential business information that must be kept secure?Check all that apply. | Bir Mühendis yeni bir ürün geliştirme üzerinde çalışmaktadır. Aşağıdakilerin hangileri güvende tutulması gereken gizli ticari bilgiler olarak kabul edilmelidir?Geçerli olan tüm seçenekleri işaretleyin. |
| Screen 46Question 5: Options70\_C\_48 | [1] Sales projections and forecasts for the new product.[2] Financial reporting data from Abbott’s Annual Report.[3] Purchasing information, such as bids for contracts for the new product.[4] Competitive information about similar products.[5] Proposals from third-party suppliers related to the new product. | [1] Yeni ürün için satış projeksiyonları ve tahminleri.[2] Abbott’ın Yıllık Raporundan alınmış finansal raporlama verileri.[3] Yeni ürün için sözleşmeler için teklifler gibi satın alma bilgileri.[4] Benzer ürünler hakkındaki rakip bilgileri.[5] Yeni ürün ile ilgili olarak üçüncü taraf tedarikçilerin teklifleri. |
| Screen 46Question 5: Feedback71\_C\_48 | Confidential Business Information is a broad category. It includes much of the business information we use and come in contact with on a daily basis. A good way to confirm whether something is confidential is to ask yourself a simple question:Is this information publicly available?If the answer is no, then the information is most certainly confidential, and you should take appropriate steps to protect it.For more information, see Section 2.1, Recognizing Confidential Business Information. | Gizli Ticari Bilgiler kapsamlı bir kategoridir. Buna, her gün kullandığımız ve karşılaştığımız ticari bilgilerinin çoğu dahildir. Bir şeyin gizli olup olmadığını teyit etmenin iyi bir yolu, kendinize basit bir soru sormaktır:Bu bilgiler kamuya açık mı?Cevap hayır ise bilgi kesin olarak gizlidir ve onu korumak için uygun önlemleri almanız gerekir.Daha fazla bilgi için bkz. Bölüm 2.1, Gizli Ticari Bilgileri Tanıma. |
| Screen 46Question 6: Scenario72\_C\_48 | The Global Data Protection Regulation (GDPR) is one of the most comprehensive privacy laws in the world. Implemented in 2018, it is the standard for privacy protection. This regulation was designed in: | Genel Veri Koruma Yönetmeliği (GDPR) dünyadaki en geniş kapsamlı gizlilik yasalarından birisidir. 2018 yılında uygulama konmuş olan bu yönetmelik gizlilik koruması için standarttır. Bu yönetmelik şurada tasarlanmıştır: |
| Screen 46Question 6: Options73\_C\_48 | [1] Canada[2] Asia[3] Europe[4] Russia[5] United States[6] Latin America | [1] Kanada[2] Asya[3] Avrupa[4] Rusya[5] Amerika Birleşik Devletleri[6] Latin Amerika |
| Screen 46Question 6: Feedback74\_C\_48 | The correct answer is Europe. In Europe, the General Data Protection Regulation (GDPR) is one of the most comprehensive privacy laws globally, and since its implementation in 2018, it has set the standard for privacy protection that other countries are trying to emulate.For more information, see Section 1.2, Legal, Regulatory and Contractual Agreements. | Doğru yanıt Avrupa’dır. Avrupa Genel Veri Koruma Düzenlemesi (GDPR), küresel olarak en kapsamlı gizlilik yasalarından biridir ve 2018 yılında uygulanmasından beri, diğer ülkelerin aynı düzeye ulaşmaya çalıştığı gizlilik koruması standardını belirlemiştir.Daha fazla bilgi için Bölüm 1.2, Yasa, Düzenleyici ve Sözleşme Gereklilikleri kapsamına bakın. |
| Screen 46Question 7: Scenario75\_C\_48 | Your colleague just completed a project that involved collecting and using personal data. He's since received a request from another department to access that data. You advise your colleague to: | İş arkadaşınız kişisel bilgi toplamayı ve kullanmayı içeren bir projeyi yeni tamamlamıştır. O zamandan beri başka bir bölümden o verilere erişmek için bir talep almıştır. İş arkadaşınıza şunu yapmasını tavsiye edersiniz: |
| Screen 46Question 7: Options76\_C\_48 | [1] Confirm the requester's identity and their need to access the information.[2] Verify that the requester is authorized to have a copy of the information.[3] Make sure that the data can be used for the requested purposes.[4] All of the above. | [1] İstek sahibinin kimliğini ve bu kişinin bilgilere erişme ihtiyacını teyit etmek.[2] İstek sahibinin bilgilerin kopyasını alma yetkisine sahip olduğunu teyit etmek.[3] Verilerin talep edilmiş amaçlar için kullanılabileceğinden emin olmak.[4] Yukarıdakilerin hepsi. |
| Screen 46Question 7: Feedback77\_C\_48 | One of the most common causes of data incidents within an organization is the improper sharing of data with unauthorized personnel. Before sharing any document or file containing sensitive data, always:* Confirm the identity of the person making the request and the person’s need to access the information.
* Check to make sure the person is authorized to have a copy of the information.
* Verify that the information can be used for the purposes they are requesting to use it for.
* Share only the amount of information required to meet the need, not more.

For more information, see Section 3.2, Sharing Sensitive Data. | Bir kuruluş içindeki veri vakalarının en yaygın nedenlerinden biri, verilerin yetkisiz personel ile uygunsuz şekilde paylaşılmasıdır. Hassas veriler içeren herhangi bir belgeyi veya dosyayı paylaşmadan önce her zaman:* İstekte bulunan kişinin kimliğini ve bu kişinin bilgilere erişme gerekçesini teyit edin.
* Kişinin bilgilerin bir kopyasını alma yetkisine sahip olup olmadığını kontrol edin.
* Talep edilen bilginin talep edilen amaç için kullanılabileceğini teyit edin.
* Fazlasını değil, yalnızca ihtiyacı karşılamak için gereken miktarda bilgiyi paylaşın.

Daha fazla bilgi için bkz. Bölüm 3.2, Hassas Bilgilerin Paylaşılması. |
| Screen 46Question 8: Scenario78\_C\_48 | You are a Sales Representative visiting a clinic in your area. While waiting in the reception area, you accidentally misplace sensitive documents containing a patient's protected health information. What do you do? | Siz, bölgenizdeki bir kliniği ziyaret etmekte olan bir Satış Temsilcisisiniz. Resepsiyon alanında beklerken, bir hastanın korunan sağlık bilgilerini içeren hassas belgeleri yanlış yere koyarsınız. Ne yaparsınız? |
| Screen 46Question 8: Options79\_C\_48 | [1] Notify the clinic's privacy officer.[2] Contact your supervisor.[3] Report the incident to OEC or a member of the Global Privacy team. | [1] Kliniğin gizlilik görevlisine haber vermek.[2] Amiriniz ile iletişime geçmek.[3] Vakayı Etik ve Tam Uyum Ofisine veya Global Gizlilik ekibinin bir üyesine bildirmek. |
| Screen 46Question 8: Feedback80\_C\_48 | In response to any inadvertent disclosure of a patient’s protected health information, you should immediately report the incident to:* OEC or a member of the Global Privacy team.

For more information, see Section 3.4, Responding to Improper Disclosures. | Bir hastanın korunan sağlık bilgilerinin yanlışlıkla açıklanması karşısında vakayı hemen aşağıdakilerin her ikisine de bildirmeniz gerekir:* Etik ve Tam Uyum Ofisine veya Global Gizlilik ekibinin bir üyesi.

Daha fazla bilgi için bkz. Bölüm 3.4, Uygunsuz İfşalara Müdahale. |
| Screen 46Question 9: Scenario81\_C\_48 | While traveling to work on the train, you accidentally leave your laptop containing sensitive work documents at your seat and exit the train. You realize your mistake when you reach your office and frantically search for your laptop, but it is nowhere to be found. What should you do first? | Trenle işe giderken, hassas iş bilgileri içeren dizüstü bilgisayarınızı kazara koltuğunuzda unutuyorsunuz ve trenden çıkıyorsunuz. Ofisinize vardığınız zaman hatanızı fark edip dizüstü bilgisayarınızı arıyorsunuz ama hiçbir yerde bulamıyorsunuz. Önce ne yapmalısınız? |
| Screen 46Question 9: Options82\_C\_48 | [1] Call the train company and ask if someone turned in your laptop.[2] Go back to the train station and search for your laptop.[3] Contact your local Global Service Desk. | [1] Tren şirketini aramak ve birisinin dizüstü bilgisayarınızı onlara getirip getirmediğini sormak.[2] Tren istasyonuna geri gitmek ve dizüstü bilgisayarınızı aramak.[3] Yerel Global Servis Masanız ile iletişime geçmek. |
| Screen 46Question 9: Feedback83\_C\_48 | If you believe that sensitive information may have been compromised, such as through a lost or stolen laptop, please contact your local Global Service Desk immediately.For more information, see Section 3.4, Reporting a Data Incident. | Kaybolan veya çalınan bir dizüstü bilgisayar yüzünden hassas verilerin tehlikeye girmiş olabileceğine inandığınız takdirde lütfen hemen yerel Global Servis Masanız ile iletişime geçin.Daha fazla bilgi için bkz. Bölüm 3.4, Bir Veri Vakasının Bildirilmesi. |
| Screen 46Question 10: Scenario84\_C\_48 | You should only use personal information:Check all that apply. | Kişisel bilgileri yalnız şu şekilde kullanmalısınız:Geçerli olan tüm seçenekleri işaretleyin. |
| Screen 46Question 10: Options85\_C\_48 | [1] For the specific purpose for which you have been granted access.[2] According to the notice provided to the data subject.[3] According to the consent granted by the data subject. | [1] Size erişim izni verilmiş olan söz konusu amaç için.[2] Veri sahibine verilen bildirime uygun şekilde.[3] Veri sahibi tarafından verilen müsaadeye uygun şekilde. |
| Screen 46Question 10: Feedback86\_C\_48 | If you have permission to access personal information, only use it:* For the specific purpose for which you have been granted access.
* According to the notice provided to the data subject.
* According to the consent granted by the data subject.

For more information, see Section 3.1 Accessing and Using Sensitive Data. | Hassas verilere erişim izniniz varsa bunu yalnızca şu şekilde kullanın:* Size erişim izni verilmiş olan söz konusu amaç için.
* Veri sahibine verilen bildirime uygun şekilde.
* Veri sahibi tarafından verilen müsaadeye uygun şekilde.

Daha fazla bilgi için bkz. Bölüm 3.1, Hassas Verilere Erişim ve Kullanım. |
| [Screen 46](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=87_C_48) [87\_C\_48](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=87_C_48)  | All questions remain unanswered | Tüm sorular yanıtlanmamış durumdadır |
| [Screen 47](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=88_C_49) [88\_C\_49](http://www.learnex.co.uk/test/AbbottProtectSensitiveInfo/us/course/index.html?showScreen=88_C_49)  | No results are available, as you have not completed the Knowledge Check.Congratulations! You have successfully passed the Knowledge Check and completed the course.Please review your results below by clicking on each question.Once you are done, you must click the EXIT [X] icon in the course title bar before closing your browser window or browser tab.Sorry, you did not pass the Knowledge Check. Take a few minutes to review your results below by clicking on each question.When you are done, click the Retake Knowledge Check button. | Bilgi Kontrolünü tamamlamadığınız için hiçbir sonuç mevcut değil.Tebrikler! Bilgi Kontrolünü başarıyla geçtiniz ve kursu tamamladınız.Lütfen her bir soruya tıklayarak aldığınız sonuçları inceleyin.Tamamladığınızda, tarayıcı pencerenizi veya tarayıcı sekmesini kapatmadan önce kurs başlığı çubuğunda **ÇIKIŞ [X]** düğmesine tıklamalısınız.Üzgünüz, Bilgi Kontrolünü geçemediniz. Her bir soruya tıklayarak aldığınız sonuçları incelemek için birkaç dakika ayırın.Tamamladığınızda, **Bilgi Kontrolüne Yeniden Gir** düğmesine tıklayın. |
| 89\_toc\_1 | Introduction | Giriş |
| 90\_toc\_2 | Welcome | Açılış |
| 91\_toc\_3 | Objectives | Amaçlar |
| 92\_toc\_4 | Menu | Menü |
| 93\_toc\_5 | Personal Information | Kişisel Bilgiler |
| 94\_toc\_6 | Recognizing Personal Information | Kişisel Bilgileri Tanıma |
| 95\_toc\_7 | Legal, Regulatory and Contractual Requirements | Yasal, Düzenleyici ve Sözleşme Gereklilikleri |
| 96\_toc\_8 | Abbott’s Privacy by Design Principles | Abbott’ın Tasarım itibarıyla Gizlilik İlkeleri |
| 97\_toc\_9 | Review | İncele |
| 98\_toc\_10 | Confidential Business Information | Gizli Ticari Bilgiler |
| 99\_toc\_11 | Recognizing Confidential Business Information | Gizli Ticari Bilgileri Tanıma |
| 100\_toc\_12 | Cost of Not Protecting Confidential Business Information | Gizli Ticari Bilgilerin Korunmamasının Maliyeti |
| 101\_toc\_13 | Insider Information | İçeriden Bilgi |
| 102\_toc\_14 | Review | İncele |
| 103\_toc\_15 | Your Role in Protecting Sensitive Data | Hassas Bilgilerin Korunmasındaki Rolünüz |
| 104\_toc\_16 | Accessing and Using Sensitive Data | Hassas Verilere Erişim ve Kullanım |
| 105\_toc\_17 | Sharing Sensitive Data | Hassas Verilerin Paylaşılması |
| 106\_toc\_18 | Retaining and Disposing of Sensitive Data | Hassas Verilerin Saklanması ve İmhası |
| 107\_toc\_19 | Responding to Improper Disclosures | Uygunsuz İfşalara Müdahale |
| 108\_toc\_20 | Review | İncele |
| 109\_toc\_21 | Knowledge Check | Bilgi Kontrolü |
| 110\_toc\_22 | Introduction | Giriş |
| 111\_toc\_23 | Assessment | Değerlendirme |
| 112\_toc\_24 | Question 1 | 1. Soru |
| 113\_toc\_25 | Question 2 | 2. Soru |
| 114\_toc\_26 | Question 3 | 3. Soru |
| 115\_toc\_27 | Question 4 | 4. Soru |
| 116\_toc\_28 | Question 5 | 5. Soru |
| 117\_toc\_29 | Question 6 | 6. Soru |
| 118\_toc\_30 | Question 7 | 7. Soru |
| 119\_toc\_31 | Question 8 | 8. Soru |
| 120\_toc\_32 | Question 9 | 9. Soru |
| 121\_toc\_33 | Question 10 | 10. Soru |
| 122\_toc\_34 | Feedback | Geri Bildirim |
| 123\_string\_1 | The Course cannot contact the LMS. Click 'OK' to continue and review the course. Note, Course Certification may not be available. Click 'Cancel' to exit  | Kurs, LMS ile iletişim kuramıyor. Devam etmek ve kursu incelemek için ‘TAMAM’ düğmesine tıklayın. Not, Kurs Sertifikasyonu mevcut olmayabilir. Çıkış için ‘İptal’ düğmesine tıklayın  |
| 124\_string\_2 | All questions remain unanswered | Tüm sorular yanıtlanmamış durumdadır |
| 125\_string\_3 | Questions | Sorular |
| 126\_string\_4 | Question | Soru |
| 127\_string\_5 | not answered | yanıtlanmadı |
| 128\_string\_6 | That's correct! | Bu, doğru! |
| 129\_string\_7 | That's not correct! | Bu, doğru değil! |
| 130\_string\_8 | Feedback:  | Geri bildirim:  |
| 131\_string\_9 | PROTECTING SENSITIVE DATA | HASSAS VERİLERİN KORUNMASI |
| 132\_string\_10 | Knowledge Check | Bilgi Kontrolü |
| 133\_string\_11 | Submit | Gönder |
| 134\_string\_12 | Retake Knowledge Check | Bilgi Kontrolüne Yeniden Gir |
| 135\_string\_13 | Course Description: At Abbott, we frequently use sensitive data to make important business decisions. Because many of our stakeholders have concerns about how this data is collected and used, Abbott has policies and procedures in place to ensure this data is protected. This course explains what sensitive data is, why it is vital to our business, and what steps we can take to ensure we process and handle this information safely and securely. This course will take approximately 30 minutes to complete. | Kurs Tanımı: Abbott’ta, bizler önemli iş kararları vermek için sık sık hassas verileri kullanırız. Paydaşlarımızın birçoğunun bu verilerin nasıl toplandığına ve kullanıldığına dair endişeleri olduğundan, Abbott bu verilerin korunmasını sağlayacak politika ve prosedürleri uygulamaya koymuştur. Bu kurs, hassas verilerin ne olduğunu, işimiz için neden hayati önem taşıdıklarını ve bu bilgileri güvenli ve emniyetli bir şekilde işlediğimizden ve ele aldığımızdan emin olmak için için hangi önlemleri alabileceğinizi açıklamaktadır. Kursun tamamlanması yaklaşık 30 dakika sürecektir. |
| 136\_string\_14 | Menu | Menü |
| 137\_string\_15 | Resources | Kaynaklar |
| 138\_string\_16 | Reference Material | Başvuru Materyali |
| 139\_string\_17 | Audio | Ses |
| 140\_string\_18 | Exit | Çıkış |
| 141\_string\_19 | Record My Results | Sonuçlarımı Kaydet |