Zweck: Key Messages für das Verarbeiten von Informationen, die von oder im Namen von Lilly bereitgestellt werden.

Zum Zwecke unserer Arbeit umfassen Informationen sowohl vertrauliche als auch persönliche Informationen, die wir zu Geschäftszwecken verwenden. Persönliche Informationen umfassen alle Informationen, die, wenn sie alleine oder in Kombination mit anderen Informationen verwendet werden, eine Einzelperson identifizieren. Vertrauliche Informationen sind als Informationen definiert, die von der offenlegenden Partei als vertraulich oder proprietär eingestuft werden.

Bitte überprüfen Sie dies in Ihrer Organisation und leiten Sie diese Infos an Personen weiter, die derzeit von Lilly oder im Namen von Lilly bereitgestellte Informationen verarbeiten oder die sich zukünftig damit befassen werden.

Warum ist dies wichtig?

- Ihre Organisation und die Mitarbeiter sind für Lilly von hohem Wert, und Aktionen, die Sie und Ihre Mitarbeiter ausführen, sind Bestandteil der vordersten und besten Verteidigungslinie gegen die Gefährdung von Informationen.
- Der Schutz von Informationen ist für Lilly und seine Kunden von zentraler Bedeutung.

Die folgenden Key Messages, die von bewährten Vorgehensweisen der Branche abgeleitet sind, einschließlich das NIST Cybersecurity Framework, sollten in aktuelle Vorgehensweisen integriert werden, um das Risiko beim Verarbeiten von Informationen zu reduzieren.

Allgemein:

- Erstellen Sie nur im absoluten Bedarfsfall elektronische oder gedruckte Kopien von Dokumenten mit Informationen.

Elektronisches Speichern von Daten:

- Elektronische Dateien mit Informationen müssen sicher gespeichert werden.
    - Wenden Sie sich an Ihren Lilly-Kontakt, wenn externer Speicher oder Cloud-Dienste, die zuvor nicht von Ihrer Organisation offengelegt oder mit Lilly vereinbart wurden, für Informationen eingesetzt werden, die von Lilly oder im Namen von Lilly bereitgestellt wurden.
    - Zugriff auf elektronische Dateien mit Informationen sollte nur den Personen gewährt werden, die diesen unbedingt benötigen. Auch sollte der Zugriff nur im erforderlichen Umfang und nur für die erforderliche Zeit gewährt werden.
    - Der Zugriff sollte gemäß der jeweiligen Vertraulichkeitsstufe überprüft werden. Dies umfasst Speicherorte, die Sie verwalten und die von Ihren Vertragspartnern verwaltet werden.
    - Die Deaktivierung sollte zeitnah nach dem Verlassen des Unternehmens oder dann erfolgen, wenn Einzelpersonen für Ihr Geschäft nicht mehr auf die Informationen zugreifen müssen.
- Informationen dürfen an den folgenden Speicherorten/auf den folgenden Geräten ohne Genehmigung durch Lilly NICHT gespeichert werden:
    - Mobile Speichergeräte wie externe Festplatten und USB-Sticks.
    - Private Geräte der Mitarbeiter wie Laptops oder iPads.

Elektronische Datenübertragung:

- Elektronische Daten mit Informationen müssen sicher übertragen werden (gemäß der jeweiligen Vertraulichkeitsstufe). Wenden Sie sich an Ihren Lilly-Kontakt, um eine zu verwendende Übertragungsmethode abzusprechen.
- Überprüfen Sie vor dem Senden die E-Mail-Adressen der Empfänger und stellen Sie sicher, dass Sie nur Adressen von Personen mit einem Geschäftsbedarf einschließen.

- Informationen dürfen folgendermaßen NICHT übertragen werden:
    - Über externe Speichergeräte wie externe Festplatten oder USB-Sticks (ohne Genehmigung durch Lilly).
    - Über private E-Mails.

Drucken:

- Informationen sollten nicht auf privaten Druckern oder an öffentlichen Orten gedruckt werden. Wenn Sie zuhause oder extern drucken müssen, verbinden Sie einen Laptop oder Ihr genehmigtes Gerät (z. B. ein iPad) über ein Kabel oder ein drahtloses Netzwerk mit dem Drucker.

Telefonkonferenzen:

- Sollten mithilfe von Skype for Business, Cisco WebEx oder Citrix GoToMeeting durchgeführt werden. Wenden Sie sich an Ihren Lilly-Kontakt, wenn Sie ein anderes Tool verwenden möchten.
- Online-Besprechungen werden nur nach Ankündigung und vorheriger Genehmigung durch Lilly aufgezeichnet.
- Achten Sie auf Ihr Umfeld und seien Sie vorsichtig, wenn Sie über Informationen sprechen.

Physische Sicherheit:

- Gewährleisten eines sicheren Arbeitsumfelds:
    - Sperren Sie den Zugriff auf Ihren Computer JEDES Mal, wenn Sie sich von ihm entfernen.
    - Laptops und iPads werden entweder in einem abschließbaren Schrank gelagert, per Kabelschloss gesichert oder am Ende des Arbeitstags mitgenommen.
    - Schließen Sie Ihren Schreibtisch, Schränke und Spind/Büro ab, wenn Sie das Gelände am Ende eines Arbeitstags verlassen.
    - Kassen Sie keine Ausdrucke auf Druckern liegen.
    - Verwenden Sie vereinbarte Methoden für die elektronische Datenübertragung und verzichten Sie, sofern möglich, auf E-Mails, Postsendungen oder Faxe.
    - Entsorgen Sie Informationen stets auf sichere Weise (z. B. durch Schreddern).

Textnachrichten:

- In Textnachrichten werden keine Informationen von oder im Namen von Lily zur Verfügung gestellt.

Melden von Informationssicherheitsvorfällen:

- Wenden Sie sich bei einem Informationssicherheitsvorfall an Ihren für die Beziehungspflege zuständigen Manager oder Sponsor bei Lilly UND melden Sie Ihre Bedenken über die Ethik- und Compliance-Hotline bei einem internen Lilly-Zugriff oder über EthicsPoint bei einem externen Zugriff.
  Vorfälle können unter anderem Folgendes umfassen:
    - E-Mail mit Informationen, die versehentlich an einen unbeabsichtigten Empfänger gesendet wurde.
    - Laptop, Festplatte oder tragbares Speichergerät mit Informationen, der/die/das verloren oder gestohlen wurde.
    - Ein Vertragsnehmer mit Zugriff auf Informationen informiert Ihr Unternehmen über einen Vorfall.
    - Ransomware
      Wenn Sie einen Bildschirm ähnlich dem untenstehenden sehen, kann durch diese Schritte das Risiko reduziert werden:
        - Ziehen Sie das Netzwerkkabel ab oder deaktivieren Sie den WLAN-Adapter.
        - Aktivieren Sie den Ruhemodus.

Vorsicht vor Phishing-Versuchen!

- Unter Phishing versteht man die Vortäuschung einer vertrauenswürdigen Entität, um an Informationen zu gelangen. Sobald Sie auf einen unbekannten Anhang oder Link in einer E-Mail klicken, kann Ihr Computer oder das gesamte Netzwerk gefährdet sein.

- Ein Phishing-Versuch ist eine unerwartete Nachricht und enthält fast immer Folgendes:

    - Einen alarmierenden Aktionsaufruf (Beispiel: Ihre Kreditkartenzahlung ist verspätet).
    - Ein Zeitelement (Beispiel: Etwas ist innerhalb von zwei Tagen fällig).
    - Eine Konsequenz (Beispiel: Lösen Sie dieses Problem, um etwas Schlimmes zu verhindern).
    - Schlechte Grammatik und/oder Rechtschreibung.
    - DARÜBER HINAUS enthält ein Phishing Versuch immer ein Element, auf das Sie klicken sollen, beispielsweise einen Link oder Anhang.

- Bleiben Sie **r**uhig und **u**ntersuchen Sie den Vorgang. Wenn eine E-Mail verdächtig erscheint, sehen Sie sich die Nachricht genau an. Klicken Sie nicht auf Links und öffnen Sie keine Anhänge, die Sie nicht erwartet haben.

- Personen mit einer E-Mail-Adresse von Lilly sind Teil des formellen Aufklärungsprogramms zum Thema Phishing von Lilly. Die Namen von Personen, die wiederholt auf solche Links oder Anhänge klicken, werden an die dritte Partei mit der Erwartung einer Folgeschulung gesendet. Wenden Sie sich an Ihren Lilly-Kontakt, wenn Sie Fragen zum formellen Aufklärungsprogramm zum Thema Phishing von Lilly haben. Wenn Sie in einer Nachricht in Ihrem Lilly-E-Mail-Konto, die Sie für verdächtig halten, auf einen Link klicken oder einen Anhang öffnen, melden Sie dies bitte über Operation Screen Door.

Falls Sie Fragen oder Bedenken haben:

- Wenden Sie sich an Ihren Lilly-Kontakt, falls Sie Fragen oder Bedenken zu den oben erläuterten Punkten haben.
- Diese Informationen finden Sie auch im Lieferantenportal unter Protect Lilly.

15 July 2017