CHRISTIAN ALEXANDER GRAF
QUALITÄTSSICHERUNG & STATISTIK

Differential Privacy

- - -

Geschützte Datenanalysen für reale Anwendungen

In unserer heutigen Daten-getriebenen Welt wird die eigene Privatsphäre ein immer kostbareres Gut. Ein tiefes Verständnis wie man professionell personenbezogene Daten schützt und gleichzeitig nutzbringende Datenanalysen durchführt ist ein Muss. Diese Schulung vermittelt Ihnen die fortgeschrittenen Techniken der Differential Privacy (DP) – einer bahnbrechenden Methodik, die messbaren Datenschutz garantiert und gleichzeitig robuste Datenanalysen und maschinelles Lernen ermöglicht.
Der Kurs wird als zweitägiges oder dreitägiges Seminar angeboten. Die zweitägige Kompaktversion bietet einen fundierten und schnellen Einstieg in die Differential Privacy und unterstützt so eine zügige Umsetzung in Ihren Projekten.
Die dreitägige Variante bietet Ihnen einen zusätzlichen theoretischen Hintergrund, zusätzliche praktische Übungen zur Implementierung und weitere Fallstudien.

Was Sie lernen werden:

- DP-gestützte Anonymisierung: Lernen Sie DP im Verbund mit herkömmlichen Methoden (Unterdrückung, Aggregation) einzusetzen und erfahren Sie, wie DP eine nachweislich stärkere Datenschutzgarantie bietet.
- DP-Methoden in der Praxis: Erlernen Sie anhand realistischer Beispiele und praktischer Übungen den Umgang mit grundlegenden und fortgeschrittenen DP-Mechanismen, darunter Laplace- und Gauß-Rauschen, Randomized Response und Kompositionstheoreme.

- Messbare Privatsphäre und messbarer Nutzen: Lernen Sie, wichtige DP-Parameter (Epsilon, Delta) zu berechnen und zu interpretieren und den Datenschutz mit der Nützlichkeit von Daten auszubalancieren
- DP-Bibliotheken: Sie lernen, welche Methoden bestehende Open Source Bibliotheken wie OpenDP oder Google Differential Privacy Library bereitstellen und wie Sie diese in Ihren Projekten inkl. Machine Learning nutzen können.
- Risiken adäquat bewerten: Führen Sie Datenschutz-Risikobewertungen durch und wählen Sie geeignete DP-Methoden auf Grundlage der NIST DP-Guidance im Rahmen einer Fallstudie aus.

Vorteile für die Teilnehmer:

- Risiko von Datenschutzverletzungen mindern: Implementieren Sie robuste DP-Prozesse um das Risiko von Datenlecks und Re-Identifizierungsrisiken auf dem Stand der Technik zu mindern.
- Dateninnovation vorantreiben: Ermöglichen Sie einen sicheren Datenaustausch und eine sichere Zusammenarbeit unter Wahrung der Privatsphäre Ihrer Kunden und Partner.
- Wettbewerbsvorteile erzielen: Positionieren Sie sich als Vorreiter im Bereich Datenschutz und beweisen Sie Ihr Engagement für ethische und sichere Datenpraktiken.
- Vertrauen und Transparenz: Stärken Sie das Vertrauen Ihrer Kunden, indem Sie Ihr Engagement für den Schutz ihrer Privatsphäre unter Beweis stellen.

Zielgruppe:

Projektleiter für Datenanalyse und klinische Studien, Datenanalysten und Entwickler von Datenanalyse-Tools (mit Schwerpunkt auf KI- und ML-Anwendungen) sowie Software-Testmanager und Security-Experten, die für den Test und die Bewertung technischer Datenschutzmaßnahmen verantwortlich sind
Für eine erfolgreiche Teilnahme empfehlen wir Grundkenntnisse in Datenanalyse und Programmierung. Hilfreich aber nicht absolut notwendig sind Grundkenntnisse über die Funktionsweise von Datenbanken und in Stochastik.

Dauer:

Kompaktkurs – 2 Tage: Der zweitägige Kurs vermittelt alle praxisrelevanten Grundlagen der Differential Privacy. Sie analysieren sensible Daten und lernen, wie Sie ein messbares Datenschutzniveau gewährleisten.

Erweiterter Kurs – 3 Tage: Der dreitägige Kurs bietet anhand zusätzlicher Fallstudien und Übungen einen tieferen Einblick in die Theorie und Anwendung der Differential Privacy, die Implementierung robuster Datenschutzmechanismen, die Bewertung von Risiken und die Auswahl geeigneter Methoden.