J.P. Morgan Corporate Challenge®

Informationen zu Datenschutz und -verarbeitung

Name und Kontaktdaten der Verantwortlichen	JPMorgan Chase Bank, National Association 277 Park Avenue, Floor 14, New York, NY, 10172-0003 USA

Name und Kontaktdaten (Vertreter – sofern zutreffend)	JPMC EMEA Privacy JPMorgan Chase Bank, National Association Floor 18, 25 Bank Street Canary Wharf London E14 5JP, GB EMEA_DataPrivacy@jpmorgan.com
Name und Kontaktdaten (Vertreter – sofern zutreffend)	macona Werbeagentur GmbH Schultheißenweg 109, 60489 Frankfurt, Germany
Name und Kontaktdaten (Vertreter – sofern zutreffend)	On Board Experiential Marketing 3437 Jack Northrop Avenue, Los Angeles, CA 90250
Name und Kontaktdaten (Vertreter – sofern zutreffend)	:datacapo IT sports services Gmbh Am Stockert 5, D-79312 Emmendingen
Name und Kontaktdaten (Vertreter – sofern zutreffend)	Simmco Data Systems 3859 Spanish Oaks Drive, West Bloomfield, MI 48323
Zweck(e) der Verarbeitung	Registrierung von Teilnehmern sowie Leitung und Durchführung der J.P. Morgan Corporate Challenge Serie („Serie“).

CONFIDENTIAL AND PROTECTED INFORMATION FROM JPMORGAN CHASE & CO.
No reproduction or distribution without written permission from JPMorgan Chase & Co.

	Medizinische Betreuung und Unterstützung der Teilnehmer auf der Strecke und im Ziel (falls erforderlich). Werbung für die Serie oder die J.P. Morgan Unternehmensfamilie bei den Teilnehmern der Serie. Speicherung und Veröffentlichung der Rennergebnisse der Teilnehmer, Präsentation der Start- und Ergebnislisten in allen relevanten Medien, die die jeweilige Veranstaltung der Serie begleiten. Erstellung einer Rennergebnisdatenbank einschließlich einer Datenbank zur Speicherung historischer Ergebnisse.
Kategorien personenbezogener Daten	**Personenbezogene Daten**: Teilnehmer an der Serie: Vorname, Nachname, Standard-ID (nur für Mitarbeiter von JPMC), Geburtsjahr, E-Mail, Rennergebnisse, geschäftliche Telefonnummer, Name des Arbeitgebers, Adresse des Arbeitgebers, Kontaktdaten, Notfallkontaktdaten. **Sensible personenbezogene Daten**: Geschlecht.
Kategorien von Empfängern	Muttergesellschaften, verbundene Unternehmen, Zweigniederlassungen und Tochtergesellschaften der genannten Verantwortlichen, die an der Durchführung oder Unterstützung der Serie oder damit zusammenhängenden Vorgängen beteiligt sind. Dazu gehören folgende Externe Dienstleister: On Board Experiential Marketing (OBE) als zentrale Agentur für das gesamte Rennmanagement der weltweiten Serie, ausgenommen Direktmarketing für die Frankfurter Veranstaltung. OBE beauftragt den lokalen Rennveranstalter in allen 13 Städten im Auftrag von JPMorgan Chase und übernimmt die Aufsicht über die gesamte Serienplanung, einschließlich Kundenservice, Registrierungsmanagement, Finanzabgleich, Statistikreporting und Zuteilungsverfolgung. Die Macona Werbeagentur GmbH ist der geschäftsführende Veranstalter der J.P. Morgan Corporate Challenge Frankfurt, der im Auftrag von JPMorgan Chase auch für den Frankfurter Kundenservice im Umgang mit den teilnehmenden Unternehmen und Teilnehmern verantwortlich ist. Macona nimmt Fragen,

CONFIDENTIAL AND PROTECTED INFORMATION FROM JPMORGAN CHASE & CO.
No reproduction or distribution without written permission from JPMorgan Chase & Co.

	Bedenken, Feedback und Beschwerden der Teilnehmer per E-Mail und Telefon entgegen und beantwortet diese. In dieser Eigenschaft benötigen sowohl OBE als auch Macona für die Durchführung von Kundenservice und Anmeldemanagement Zugriff auf die Event-Management-Datenbank, in der die Anmeldedaten und Rennergebnisse gespeichert sind. Die :datacapo IT sports services GmbH und Simmco Data Systems sind für den Druck der Startnummern und die Rennergebnisse zuständig.
Weitergabe an Drittländer oder an eine internationale Organisation	Vereinigte Staaten von Amerika.
Aufbewahrungsfrist	Solange (i) personenbezogene Daten im Zusammenhang mit den hier dargelegten Zwecken, für die eine gültige Rechtsgrundlage besteht, erforderlich sind oder (ii) eine gesetzliche Verpflichtung (z. B. gesetzliche Aufbewahrungspflichten) zur Aufbewahrung der personenbezogenen Daten besteht. Darüber hinaus können personenbezogene Daten für die Dauer der geltenden gesetzlichen Verjährungsfrist (z. B. für den Zeitraum, in dem eine Person im Zusammenhang mit den Daten einen Rechtsanspruch geltend machen könnte) sowie für die Dauer des Zeitraums, in dem Rechtsansprüche und damit zusammenhängende Rechtsansprüche anhängig sind, aufbewahrt werden. Zuzüglich einer angemessenen Frist für die Vernichtung oder Anonymisierung der personenbezogenen Daten am Ende des jeweiligen oben genannten Zeitraums.
Mechanismen für die grenzüberschreitende Übertragung personenbezogener Daten in Drittländer	Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules- BCRs) für Übertragungen zwischen Unternehmen der J.P. Morgan Gruppe und von der Datenschutzbehörde genehmigte Mustervertragsklauseln oder andere gültige Mechanismen (z. B. Privacy Shield) für Übertragungen an Dritte, Angemessenheitsentscheidungen oder andere gültige Ausnahmen für die Übertragung personenbezogener Daten (z. B. Einwilligung).
Allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen	J.P. Morgan hat ein Programm zur Datenssicherheit entwickelt. Das Informationssicherheitsprogramm von J.P. Morgan dient folgenden Zwecken: • Gewährleistung der Sicherheit und Vertraulichkeit von Kunden- und Mitarbeiterdaten. • Schutz vor zu erwartenden Bedrohungen oder Risiken für die Sicherheit oder Integrität dieser Daten. • Verhinderung unbefugten Zugriffs auf oder die Verwendung von Daten, wodurch Kunden oder Mitarbeiter geschädigt werden könnten. • Ordnungsgemäße Speicherung, Übertragung und Löschung von

CONFIDENTIAL AND PROTECTED INFORMATION FROM JPMORGAN CHASE & CO.
No reproduction or distribution without written permission from JPMorgan Chase & Co.

	Kunden- und Mitarbeiterdaten. • Inkenntnissetzung der Mitarbeiter über ihre Verantwortung für den Schutz von Kundendaten und die Sicherheit der JPMC-Systeme. • Sicherstellung der Einhaltung der Sicherheitsrichtlinien und -standards von J.P. Morgan sowie der geltenden gesetzlichen Bestimmungen durch wichtige Drittanbieter. • Einhaltung aller Kundenbenachrichtigungsanforderungen zum Schutz von Daten. Die IT-Risiko- und -Sicherheitsrichtlinien und -standards von J.P. Morgan bilden die Grundlage des Informationssicherheitsprogramms und begründen die Regeln für den Schutz der IT-Umgebung von J.P. Morgan. Das Programm wird von J.P. Morgan auf höchster Ebene, unter anderem vom Global Technology Operating Committee, welches das Programm überwacht, genau kontrolliert. Dieser Ausschuss setzt sich aus Vertretern der einzelnen Geschäftsbereiche und der entsprechenden Aufgabenbereiche im Unternehmen zusammen. Der Prüfungsausschuss des Vorstands überprüft und genehmigt das Programm jährlich, wobei interne und externe Revisoren die IT-Programme und -Prozesse von J.P. Morgan laufend überprüfen. Das Informationssicherheitsprogramm konzentriert sich auf die folgenden Schlüsselbereiche: • Cyber-Security Maßnahmen Bedrohungsmanagement • Identitäts- und Zugriffsmanagement • Notfallmanagement • physische Sicherheit, Nachforschungen und Krisenmanagement • Datenschutz • Überwachung von externen Dienstleistern • Produktionssicherung • Risikobewertung • Compliance -Maßnahmen und -Reporting • Schulung und Sensibilisierung. J.P. Morgan verfügt darüber hinaus über ein Informationstechnologie (IT)-Risikomanagementsystem, das auf die Anforderungen der Finanzaufsichtsbehörden und Datenschutzgesetze und -vorschriften zugeschnitten ist. Das System deckt die folgenden Bereiche ab: • Informationstechnologie-Risikomanagement • Informationssicherheitsmanagement • Informationstechnologie-Zugriffsmanagement • Informationstechnologie-Notfallmanagement

CONFIDENTIAL AND PROTECTED INFORMATION FROM JPMORGAN CHASE & CO.
No reproduction or distribution without written permission from JPMorgan Chase & Co.

	• Informationstechnologiebereitstellung • Informationstechnologie-Betriebsmanagement • Informationstechnologie-Asset und Konfiguration. Diese Richtlinien und Standards begründen Kontrollen zur Sicherung von technischen Systemen und Datenübertragungen, einschließlich: • Anwendungssicherheitsstandards, die die Sicherheitsanforderungen während der Entwicklung und Verwaltung des Systems berücksichtigen • Richtlinien und Standards für die Datenspeicherung und -vernichtung, die Klassifizierung von Daten und Maßnahmen zur Verhinderung unbefugter Zugriffe • Standards für die Behandlung und den Schutz personenbezogener Daten einschließlich Verschlüsselung • Richtlinien und Standards zur physischen Sicherheit von Rechenzentren, Betriebszentren, sonstigen Gebäuden und Anlagen • Ein Notfallprogramm, das regelmäßig getestet und aktualisiert wird, damit im Falle eines Notfalls kritische Anwendungen und Systeme weiterhin funktionieren • Überwachung der Systeme, um sie vor Viren und anderen Bedrohungen zu schützen und eine schnelle Wiederherstellung nach Vorfällen zu ermöglichen • Gewährleistung, dass externe Dienstleister, die mit der Verarbeitung personenbezogener Daten beauftragt werden, die Sicherheitsrichtlinien und -standards von J.P. Morgan einhalten.

CONFIDENTIAL AND PROTECTED INFORMATION FROM JPMORGAN CHASE & CO.
No reproduction or distribution without written permission from JPMorgan Chase & Co.