FIFA®

Datenschutzreglement

Ausgabe Oktober 2019

Fédération Internationale de Football Association

Präsident:	Gianni Infantino
Generalsekretärin:	Fatma Samoura
Adresse:	FIFA FIFA-Strasse 20 Postfach 8044 Zürich Schweiz
Telefon:	+41 (0)43 222 7777
Internet:	FIFA.com

FIFA-Datenschutzreglement

Ausgabe Oktober 2019

INHALT *Seite*

1 Präambel 4
2 Definitionen 4
3 Anwendungsbereich 7
4 Datenverarbeitung 8
1. Grundsätze 8
2. Besondere Kategorien personenbezogener Daten 10
5 Rechte betroffener Personen 10
6 Übermittlung personenbezogener Daten an Drittparteien/ Datenverarbeitung durch Drittparteien 12
7 Grenzüberschreitende Offenlegung 13
1. Grundsätze 13
2. Fehlen eines angemessenen Datenschutzes im Ausland 13
8 Organisationsinterne Verarbeitungsrichtlinien 13
1. Pflichten 13
2. Prozessverantwortlicher 14
3. Datenverzeichnis 14
4. Kontrollen durch den Prozessverantwortlichen 14
9 Anforderungen an die Informationssicherheit 14
10 Datensicherheitsvorfall 15
11 Datenschutzbeauftragter (DSB) 15
12 Schlussbestimmungen 16
1. Offizielle Sprachen 16
2. Sanktionen 16
3. Inkrafttreten 16

Hinweis:
Beziehen sich die Begriffe auf natürliche Personen, sind Mann und Frau gleichgestellt. Der Einfachheit halber wird nur die männliche Form verwendet. Begriffe in der Einzahl schliessen die Mehrzahl mit ein und umgekehrt.

1 Präambel

Die FIFA legt grossen Wert darauf, die Persönlichkeitsrechte jedes Einzelnen, mit dem sie interagiert, zu achten und personenbezogene Daten entsprechend zu schützen. Dieses Reglement definiert die Grundsätze der Datenverarbeitung, die Übermittlung von Daten innerhalb sowie zwischen der FIFA, deren Mitgliedsverbänden und sämtlichen Organisationen, auf die dieses Reglement anwendbar ist, den Standard zum Schutz besonderer Kategorien personenbezogener Daten sowie die Rechte aller betroffenen Personen.

Bei ihrer operativen Tätigkeit verarbeitet die FIFA verschiedene Arten personenbezogener Daten. Mit diesem Reglement will die FIFA:

- einen Standard für die Verarbeitung personenbezogener Daten festlegen,
- Vorkehrungen treffen, um Verletzungen von Persönlichkeitsrechten durch eine unsachgemässe Verarbeitung personenbezogener Daten zu vermeiden.

Neben diesem Reglement sind auch alle massgebenden Datenschutzgesetze anwendbar, die insbesondere auch dann einzuhalten sind, wenn sie strengere Vorschriften vorsehen als dieses Reglement.

2 Definitionen

In diesem Reglement gelten folgende Begriffsbestimmungen:

Anwendbare Datenschutzgesetze
Das Schweizer Bundesgesetz über den Datenschutz (DSG) und, soweit für eine bestimmte Verarbeitung personenbezogener Daten massgebend, alle anderen anwendbaren Datenschutzgesetze einschliesslich sämtlicher Änderungen.

Besondere Kategorien personenbezogener Daten
Alle personenbezogenen Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder eine Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung genetischer oder biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person.

Betroffene Person
Identifizierte oder identifizierbare natürliche Person, deren Daten verarbeitet werden. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten, einer Online-Kennung oder einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert oder ausgesondert werden kann.

Datensicherheitsvorfall
Jede Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten, die für die FIFA, eine andere Organisation oder eine betroffene Person ein Risiko darstellen kann.

Drittpartei
Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die weder als Organisation noch als betroffene Person gilt, sowie Personen, die unter der unmittelbaren Verantwortung einer Organisation befugt sind, personenbezogene Daten zu verarbeiten.

DSG
Schweizer Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SR 235.1) einschliesslich sämtlicher Änderungen.

EDÖB
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter.

Einwilligung
Jede freiwillig, konkret, informiert und unmissverständlich abgegebene Willensbekundung einer betroffenen Person in Form einer Erklärung oder einer sonstigen eindeutigen Bestätigung, mit der sie ihr Einverständnis mit der Verarbeitung sie betreffender personenbezogener Daten zum Ausdruck bringt.

FIFA
Fédération Internationale de Football Association. Im Sinne dieses Reglements fallen auch die FIFA-Tochtergesellschaften unter den Begriff „FIFA“.

FIFA-Tochtergesellschaft
Juristische Person, die ganz oder teilweise der FIFA gehört oder von dieser kontrolliert wird (indem die FIFA die Mehrheit besitzt).

Mitgliedsverband
Nationaler Fussballverband, der vom FIFA-Kongress in die FIFA aufgenommen wurde.

Offenlegung/offenlegen
Übermittlung personenbezogener Daten oder Bereitstellen des Zugriffs auf personenbezogene Daten, z. B. durch das Gewähren der Einsichtnahme, Weitergeben oder Veröffentlichen.

Organisationseinheit
Mit „Organisation" ist die FIFA, ein beliebiger Mitgliedsverband oder ein Mitglied eines Mitgliedsverbands gemeint, während sich „Einheit" auf einen einzelnen hierarchischen Bereich der internen Struktur einer Organisation bezieht.

Personenbezogene Daten
Sämtliche Informationen, die sich auf eine betroffene Person beziehen.

Profiling
Jede Art der automatisierten Verarbeitung personenbezogener Daten, die personenbezogene Daten zur Bewertung bestimmter persönlicher Aspekte zu einer natürlichen Person verwendet, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person.

Prozessverantwortlicher
Person, die gemäss hierarchischer Organisation der FIFA, der Mitgliedsverbände und deren Mitglieder für eine Verarbeitung verantwortlich ist. Wenn der Prozessverantwortliche nicht bestimmt wurde oder werden kann, gilt als Prozessverantwortlicher die Person, die für die Organisationseinheit verantwortlich ist, die die Verarbeitung für ihre Zwecke oder zur Unterstützung ihrer Tätigkeiten nutzt.

Reglement
Vorliegendes FIFA-Datenschutzreglement.

Verarbeitung/verarbeiten
Jeder Vorgang oder jede Reihe von Vorgängen mit personenbezogenen Daten oder Sätzen personenbezogener Daten – ob mit oder ohne automatisierte Verfahren – wie das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Ändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermitteln, Verbreiten oder Bereitstellen in anderer Form, Abgleichen oder Verknüpfen, Einschränken, Löschen oder Vernichten.

3 Anwendungsbereich

Dieses Reglement findet uneingeschränkt auf alle Tätigkeiten der FIFA Anwendung.

Dieses Reglement ist auch auf alle Mitgliedsverbände und ihre Mitglieder anwendbar. Die Mitgliedsverbände müssen dafür sorgen, dass sie selbst und ihre Mitglieder dieses Reglement einhalten. Auf Mitgliedsverbände und ihre Mitglieder findet dieses Reglement aber nur insofern Anwendung, als sie:

- für, im Auftrag von oder mit der FIFA personenbezogene Daten verarbeiten,
- personenbezogene Daten mit der FIFA, anderen Mitgliedsverbänden, deren Mitgliedern oder mit Drittparteien im Auftrag der FIFA austauschen oder diesen übermitteln,
- Infrastruktur nutzen, die die FIFA ihren Mitgliedsverbänden und deren Mitgliedern zwecks Verarbeitung personenbezogener Daten zur Verfügung stellt.

Nicht anwendbar ist dieses Reglement hingegen, wenn Mitgliedsverbände und ihre Mitglieder personenbezogene Daten unter folgenden kumulativen Voraussetzungen verarbeiten:

- mit ihrer eigenen Infrastruktur
- für ihre eigenen Zwecke
- eigenständig

4 Datenverarbeitung

1. Grundsätze

Die FIFA verarbeitet personenbezogene Daten gemäss folgenden Grundsätzen. Personenbezogene Daten müssen:

- gegenüber der betroffenen Person rechtmässig, nach Treu und Glauben sowie transparent verarbeitet werden,

Beispiel: *Personenbezogene Daten werden rechtmässig, nach Treu und Glauben sowie transparent verarbeitet, wenn ein Veranstaltungsticket anhand des Vornamens, des Namens, des Geschlechts, des Geburtsdatums und der Postadresse einem Käufer zugewiesen und diesem zugestellt wird, sofern dem Käufer mitgeteilt wurde, welche personenbezogenen Daten für welchen Zweck genutzt werden.*

- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht auf eine Art und Weise verarbeitet werden, die diesen Zwecken entgegensteht. Die Weiterverarbeitung zu Archivierungszwecken im öffentlichen Interesse, zwecks wissenschaftlicher oder historischer Forschung oder für statistische Zwecke gilt als mit den ursprünglichen Zwecken vereinbar,

Beispiel: *Wenn für den Kauf eines Veranstaltungstickets allein zwecks Ausstellung dieses Tickets Daten erhoben werden und der Käufer nicht über eine weitere Verwendung seiner personenbezogenen Daten informiert wurde, dürfen diese personenbezogenen Daten nicht für andere Zwecke, wie den Weiterverkauf an einen offiziellen Sponsor für Marketingzwecke, verwendet werden.*

- angemessen, erheblich und in Bezug auf die Zwecke, für die sie verarbeitet werden, auf das notwendige Mass beschränkt sein,

Beispiel: *Alle personenbezogenen Daten, die verarbeitet werden, müssen dem Zweck dienen, für den sie erhoben wurden. Neben den für den ursprünglichen Zweck nötigen Daten dürfen keine weiteren personenbezogenen Daten erhoben und weiterverarbeitet werden.*

- sachlich richtig und wo nötig auf dem neusten Stand sein. Es sind alle zumutbaren Massnahmen zu ergreifen, damit personenbezogene Daten, die in Bezug auf die Zwecke, für die sie verarbeitet werden, unrichtig sind, unverzüglich gelöscht oder berichtigt werden,

Beispiel: *Alle personenbezogenen Daten müssen sachlich richtig sein. Betroffene Personen können verlangen, dass unrichtige personenbezogene Daten berichtigt werden. Soweit möglich und zweckmässig kann der Prozessverantwortliche Instrumente vorsehen, über die die betroffenen Personen auf ihre personenbezogenen Daten zugreifen, diese überprüfen und berichtigen können.*

- derart gespeichert werden, dass betroffene Personen nur so lange, wie es für die Zwecke erforderlich ist, identifiziert werden können. Personenbezogene Daten dürfen länger gespeichert werden, solange diese ausschliesslich zu Archivierungszwecken im öffentlichen Interesse, zwecks wissenschaftlicher oder historischer Forschung oder für statistische Zwecke verarbeitet werden und zum Schutz der Rechte und Freiheiten der betroffenen Personen, wie von den anwendbaren Datenschutzgesetzen vorgeschrieben, geeignete technische und organisatorische Massnahmen getroffen werden,

Beispiel: *Der Prozessverantwortliche muss gegebenenfalls zusammen mit anderen Organisationseinheiten die maximale Aufbewahrungsdauer personenbezogener Daten festlegen und den entsprechenden Beschluss dokumentieren.*

- mithilfe geeigneter technischer und organisatorischer Massnahmen auf eine Art und Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschliesslich des Schutzes vor unbefugter oder unrechtmässiger Verarbeitung sowie vor einem versehentlichen Verlust oder einer versehentlichen Zerstörung oder Schädigung.

Beispiel: *Geeignete organisatorische Massnahmen können etwa die Einrichtung interner Prozesse zur Einhaltung der anwendbaren Datenschutzgesetze sein, u. a. durch die vertragliche Verpflichtung von ehrenamtlichen Helfern, Angestellten und Auftragnehmern zur rechtmässigen Verarbeitung von Daten, den Erlass interner Vorschriften sowie die Durchführung von Sensibilisierungskampagnen und Schulungen.*

- Zugriff auf personenbezogene Daten dürfen nur solche Personen haben, die diese Daten für ihre Arbeit benötigen (Grundsatz „Kenntnis nur, wenn nötig“).

Beispiel: *Der Zugriff auf Personaldaten ist auf Personen zu beschränken, die für das Personalwesen Daten bearbeiten (Personalabteilung).*

- Jede Organisation muss dafür sorgen, dass die gesamte Infrastruktur, die für die Verarbeitung personenbezogener Daten genutzt wird, gemäss neustem Stand mit wirtschaftlich verhältnismässigen technischen und organisatorischen Massnahmen geschützt wird, wobei die Risiken einer unrechtmässigen Verarbeitung personenbezogener Daten für die betroffenen Personen zu berücksichtigen sind.

2. Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogener Daten, d. h. Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder eine Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person, sind vor unbefugtem Zugriff besonders zu schützen.

Alle Personen, die besondere Kategorien personenbezogener Daten verarbeiten, sind ausdrücklich auf die Notwendigkeit eines streng vertraulichen Verfahrens mit besonderen Kategorien personenbezogener Daten hinzuweisen.

Besondere Kategorien personenbezogener Daten dürfen nur an Drittparteien übermittelt werden, wenn dafür rechtliche Gründe oder eine ausdrückliche Einwilligung der betroffenen Person vorliegen.

5 Rechte betroffener Personen

Betroffene Personen haben gemäss den anwendbaren Datenschutzgesetzen folgende Rechte:

- Recht auf Auskunft über die Erhebung und Nutzung personenbezogener Daten

Beispiel: *Vor der Erhebung personenbezogener Daten muss der betroffenen Person mitgeteilt werden, welche personenbezogenen Daten für welche Zwecke erhoben werden. Die entsprechenden Informationen müssen einfach abrufbar sein oder öffentlich vorliegen, leicht zugänglich sowie klar verständlich und einfach geschrieben sein.*

- Recht auf Zugriff auf die personenbezogenen Daten, die von ihnen erfasst wurden. Ein Antrag auf Zugriff muss binnen 30 Tagen eingereicht werden. Betroffene Personen, die Zugriff auf ihre Daten beantragen, müssen sich identifizieren können. Die Art der Identifizierung muss in Bezug auf die personenbezogenen Daten, auf die eine betroffene Person Zugriff verlangt, verhältnismässig sein. Soweit machbar, technisch angemessen und wirtschaftlich verhältnismässig sollten alle betroffenen Personen über eine Web-Schnittstelle, die über ausreichende Sicherheits- und Authentifizierungsmechanismen verfügt, Zugriff auf ihre Daten haben.

Betroffene Personen dürfen Auskunft darüber verlangen, welche personenbezogenen Daten die fragliche Organisation für welche Zwecke verarbeitet. Um zu gewährleisten, dass die Person, die Auskunft verlangt, wirklich die betroffene Person ist, die sie vorgibt, sind Authentifizierungsmechanismen vorzusehen. Für den Zugriff auf sensible Daten müssen strengere Authentifizierungsmechanismen bestehen. So kann etwa eine Kopie eines offiziellen Identifikationsdokuments (staatlich ausgestellter Personalausweis, Reisepass, Fahrausweis) verlangt werden. Auch die Übermittlung eines solchen Identitätsnachweises muss ausreichend gesichert werden. Für den Zugriff auf weniger sensible Daten innerhalb einer Web-Applikation reichen hingegen die Logindaten der betroffenen Person. In diesem Fall sollte den betroffenen Personen in der Web-Applikation Zugriff auf ihre personenbezogenen Daten gewährt werden. Allgemein gilt, dass der Zugriff auf personenbezogene Daten in einer Web-Applikation (Forum, Web-Shop mit Kundenberechtigungsnachweis etc.) den Zugriffsprozess vereinfachen kann.

- Recht auf Berichtigung, wenn von ihnen erfasste personenbezogene Daten falsch oder unvollständig sind.

Betroffene Personen dürfen ihren Namen, ihre Adresse etc. oder andere personenbezogene Daten ändern, wenn diese aus irgendeinem Grund falsch erfasst wurden.

- Recht auf Vergessen, d. h., Recht zu verlangen, dass sämtliche personenbezogenen Daten, die eine Organisation von ihnen besitzt, gelöscht werden.

Bei der Verarbeitung personenbezogener Daten sind Instrumente vorzusehen, die personenbezogene Daten entweder unwiderruflich löschen oder anonymisieren. Auch pseudonymisierte Daten sind als personenbezogene Daten zu betrachten.

- Recht auf Einschränkung (d. h. Verhinderung) der Verarbeitung personenbezogener Daten gemäss den anwendbaren Datenschutzgesetzen.

Wenn eine betroffene Person gegen eine Organisation rechtliche Schritte einleiten will, kann sie eine Einschränkung der Nutzung personenbezogener Daten verlangen, bis die Rechtmässigkeit der Verarbeitung der fraglichen Daten bestätigt oder verneint wurde.

- Recht auf Übertragung von Daten (d. h. Recht auf Erhalt einer Kopie personenbezogener Daten zur Nutzung bei anderen Dienstleistungserbringern oder Organisationen).

Betroffene Personen haben das Recht, eine Kopie ihrer personenbezogenen Daten in einem maschinenlesbaren Format zu exportieren. Wenn eine Web-Applikation Zugriff auf personenbezogene Daten bietet, kann es sinnvoll sein, auf der entsprechenden Seite eine Exportfunktion für die abgerufenen Daten vorzusehen.

- Recht, bei der zuständigen Aufsichtsbehörde und den zuständigen Gerichten gemäss den anwendbaren Datenschutzgesetzen Beschwerde einzureichen.

- Recht auf Genugtuung und, sofern gegeben, auf Schadenersatz bei Verstössen gegen die anwendbaren Datenschutzgesetze.

- Recht, eine menschliche Überprüfung gemäss den anwendbaren Datenschutzgesetzen zu verlangen, wenn die Verarbeitung personenbezogener Daten auch automatisierte Entscheidungen und Profiling umfasst und die fragliche automatisierte Entscheidung gegenüber der betroffenen Person rechtliche Wirkung entfaltet.

6 Übermittlung personenbezogener Daten an Drittparteien/ Datenverarbeitung durch Drittparteien

Personenbezogene Daten dürfen an Drittparteien übermittelt werden, sofern die Verarbeitung gemäss diesem Reglement erfolgt und weder gesetzliche noch vertragliche Geheimhaltungspflichten eine solche Übermittlung verbieten. Die Übermittlung personenbezogener Daten an Drittparteien muss derart gestaltet sein, dass die jeweilige Drittpartei die Daten gemäss den Anweisungen des Übermittlers verarbeitet.

7 Grenzüberschreitende Offenlegung

1. Grundsätze
Eine grenzüberschreitende (d. h. über die Schweiz hinaus) Offenlegung personenbezogener Daten (einschliesslich der Gewährung eines Fernzugriffs) ist zulässig, sofern im fraglichen Land gemäss der Staatenliste des EDÖB ein angemessener gesetzlicher Datenschutz gewährleistet ist.

2. Fehlen eines angemessenen Datenschutzes im Ausland
Eine grenzüberschreitende Offenlegung personenbezogener Daten in Ländern ohne angemessenen Datenschutz ist gestattet, sofern alternativ:

a) dieses Reglement eingehalten wird,
b) mit dem Empfänger vertragliche oder anderweitig rechtswirksame hinreichende Garantien vereinbart wurden,
c) die betroffene Person im Einzelfall eingewilligt hat,
d) die Verarbeitung personenbezogener Daten in unmittelbarem Zusammenhang mit dem Abschluss oder der Ausführung eines Vertrags steht und es sich um personenbezogene Daten des Vertragspartners handelt,
e) es zur gerichtlichen Durchsetzung von Rechtsansprüchen erforderlich ist,
f) die Offenlegung innerhalb derselben juristischen Person oder desselben Unternehmens erfolgt und die anwendbaren internen Datenschutzrichtlinien angemessenen Schutz bieten.

8 Organisationsinterne Verarbeitungsrichtlinien

1. Pflichten
Jede Organisation muss die nötigen technischen und organisatorischen Massnahmen ergreifen, um die Einhaltung dieses Reglements und der anwendbaren Datenschutzgesetze zu gewährleisten, und dafür sorgen, dass ihre Mitarbeiter geschult werden und dieses Reglement einhalten. Sie muss die Art, den Zweck und die Gründe der von ihr vorgenommenen Verarbeitung, die zwecks Einhaltung dieses Reglements getroffenen technischen und organisatorischen Massnahmen sowie alle anderen für eine bestimmte Verarbeitung massgebenden Informationen dokumentieren.

2. Prozessverantwortlicher
Jede Organisation muss interne Richtlinien erlassen, damit für jede Verarbeitung personenbezogener Daten ein Prozessverantwortlicher feststeht.

3. Datenverzeichnis
Jede Organisation muss ein Verzeichnis über ihre Verarbeitungsprozesse führen, das folgende Angaben beinhaltet:

- Name und Kontaktangaben der für die Verarbeitung zuständigen Person
- Beschreibung der Verarbeitung
- Zweck der Verarbeitung
- Beschreibung der Kategorien betroffener Personen
- Beschreibung der Kategorien personenbezogener Daten
- besondere Kategorien personenbezogener Daten
- Kategorien von Empfängern
- Bezeichnung von Drittländern (d. h. Gerichtsbarkeiten und internationale Organisationen ausserhalb der Schweiz)
- Kategorien von Empfängern in Drittländern
- Sicherheitsmassnahmen bei Empfängern in Drittländern
- Name des Auftragsverarbeiters
- Titel/Version des Vertrags mit dem Auftragsverarbeiter
- Dauer der Datenspeicherung
- technische und organisatorische Sicherheitsmassnahmen

4. Kontrollen durch den Prozessverantwortlichen
Der Prozessverantwortliche muss die Angaben im Datenverzeichnis regelmässig überprüfen.

9 Anforderungen an die Informationssicherheit

Alle personenbezogenen Daten müssen gegen das Risiko eines Verlusts der Vertraulichkeit, Integrität und Verfügbarkeit geschützt werden. Organisationen müssen alle nötigen, wirtschaftlich verhältnismässigen technischen und organisatorischen Massnahmen gemäss neustem Stand ergreifen und interne Richtlinien zur Informationssicherheit erlassen und durchsetzen.

10 Datensicherheitsvorfall

Jeder Verlust der Vertraulichkeit, Integrität und Verfügbarkeit, die für die FIFA, eine andere Organisation oder eine betroffene Person ein Risiko darstellen kann, ist als Datensicherheitsvorfall zu behandeln. Jeder Datensicherheitsvorfall, der in den Anwendungsbereich dieses Reglements fällt, muss per E-Mail (alert@fifa.org) gemeldet werden.

Jede Organisation muss ein eigenes Team einsetzen, das gegen Datensicherheitsvorfälle vorgeht. Alle Organisationen und Datenbesitzer müssen klare Verfahren festlegen, damit Datensicherheitsvorfälle zuerst intern und schliesslich der FIFA unverzüglich gemeldet werden. Wenn eine andere Organisation einen Datensicherheitsvorfall einer Behörde melden muss, die gemäss den anwendbaren Datenschutzgesetzen für den entsprechenden Vorfall zuständig ist, muss auch die FIFA entsprechend unterrichtet werden.

11 Datenschutzbeauftragter (DSB)

Die FIFA hat einen DSB eingesetzt. Betroffene Personen, die im Zusammenhang mit der Verarbeitung personenbezogener Daten im Anwendungsbereich dieses Reglements Rechte ausüben möchten, können sich per E-Mail (dataprotection@fifa.org) an den DSB wenden.

Der DSB organisiert, analysiert und kontrolliert unabhängig die Einhaltung der Datenschutzvorschriften und insbesondere dieses Reglements.

12 Schlussbestimmungen

1. Offizielle Sprachen

Im Falle unterschiedlicher Auslegung des deutschen, englischen, französischen oder spanischen Texts dieses Reglements ist der englische Text massgebend.

2. Sanktionen

Jeder Verstoss gegen dieses Reglement kann Sanktionen nach Massgabe der anwendbaren Datenschutzgesetze, der FIFA-Statuten und aller anderen FIFA-Reglemente nach sich ziehen.

3. Inkrafttreten

Dieses Reglement wurde vom FIFA-Rat am 24. Oktober 2019 genehmigt und trat sofort in Kraft.

Shanghai, 24. Oktober 2019

Für den FIFA-Rat:

President:
Gianni Infantino

Generalsekretärin:
Fatma Samoura

MIX
Paper from
responsible sources
FSC® C006844
FSC
www.fsc.org

Fédération Internationale de Football Association