

Dienstvereinbarung über die audiovisuell-elektronische Beobachtung an der Humboldt-Universität zu Berlin

zwischen
dem Gesamtpersonalrat
und
der Humboldt-Universität zu Berlin

- Präambel
- § 1 Grundsätze
- § 2 Audiovisuell-elektronische Einrichtungen für Beobachtungen
- § 3 Antrag auf Betrieb der audiovisuell-elektronischen Beobachtungsanlage
- § 4 Auswertung der Aufzeichnungen, Sperrung und Löschung
- § 5 Liste der in Betrieb befindlichen elektronischen Einrichtungen für Beobachtungen
- § 6 Sonderregelungen für Webcams
- § 7 Sonderregelungen für den Einsatz in der multimedialen Lehre und Forschung
- § 8 Rechtsfolgen bei Verstößen
- § 9 Übergangsregelungen

Präambel

Zum Schutz der Beschäftigten der Humboldt-Universität zu Berlin (hauptberufliches Personal und studentische Beschäftigte gem. § 121 BerIHG) und zur Sicherung des Eigentums und Besitzes der Humboldt-Universität zu Berlin sehen die Universitätsleitung und die Personalvertretungen der Humboldt-Universität zu Berlin Regelungsbedarf bei der elektronischen Beobachtung und Sicherung von Räumlichkeiten und Plätzen, die in den Verantwortungsbereich der Humboldt-Universität zu Berlin fallen. In dieser Dienstvereinbarung soll der Einsatz aller Anlagen, die zu einer solchen Beobachtung geeignet sind, geregelt werden. Dabei sind stets die Grundsätze der Verhältnismäßigkeit und der Erforderlichkeit gemäß § 31 b Berliner Datenschutzgesetz (BlnDSG) zu beachten.

§ 1 Grundsätze

- (1) Die audiovisuell-elektronische Beobachtung sowie die Errichtung und der Betrieb der dafür notwendigen Anlagen erfolgt unter Beachtung des Grundsatzes der Datenvermeidung und Datenminimierung gemäß § 5 a BlnDSG.
- (2) Um das Sicherheitsbedürfnis sowie das Recht auf informationelle Selbstbestimmung der Beschäftigten der Humboldt-Universität zu Berlin nicht durch die Schutzmaßnahmen zu gefährden, ist der Zugang zu den mit Hilfe der elektronischen Beobachtungsanlagen gewonnenen Daten gemäß § 5 Abs. 1 Ziffer 1 BlnDSG zu minimieren.
- (3) Vor Inbetriebnahme einer elektronischen Beobachtungsanlage ist vom Betreiber ein Sicherheitskonzept zu erstellen. Die Inhalte des Sicherheitskonzeptes sind in §§ 3 und 4 der Dienstvereinbarung audiovisuell-elektronische Beobachtung dargelegt.
- (4) Die mit Hilfe der elektronischen Beobachtung gewonnenen Erkenntnisse dürfen nicht zur arbeitsrechtlichen Leistungskontrolle herangezogen werden.

§ 2 Audiovisuell-elektronische Einrichtungen für Beobachtungen

- (1) Audiovisuell-elektronische Einrichtungen für Beobachtungen sind alle Geräte, die geeignet sind, Bild und/oder Ton zu übertragen bzw. aufzuzeichnen.
- (2) Regelfall ist die Videobeobachtungsanlage mit Aufzeichnungsmöglichkeit, wobei die Aufzeichnungen nur bei Zwischenfällen nach den Regeln dieser Dienstvereinbarung ausgewertet werden.

- (3) Ferner ist das so genannte verlängerte Auge möglich (Videobeobachtung ohne Aufzeichnung mit in der Regel permanenter Beobachtung durch eine Person an einem Monitor).
- (4) Elektronisch überwachte Bereiche werden deutlich gekennzeichnet (**Anlage 1**).
- (5) Anlagen, die für Videokonferenzen und Teleteaching bestimmt sind, dürfen nur für diese Zwecke eingesetzt werden. Der Einsatz zu Überwachungszwecken ist unzulässig.
- (6) Bereiche mit Videokonferenz- oder Teleteachingausrüstung werden entsprechend gekennzeichnet (**Anlage 2**).

§ 3 Antrag auf Betrieb der audiovisuell-elektronischen Beobachtungsanlage

- (1) Der Betrieb einer elektronischen Beobachtungsanlage wird durch die jeweilige Struktureinheit (Fakultät, Institut, Abteilung, Zentraleinrichtung) bei dem/der Behördlichen Datenschutzbeauftragten der Universität unter rechtzeitiger Einreichung des Sicherheitskonzeptes und der Darlegung der Erforderlichkeit und der Verhältnismäßigkeit beantragt (Mustersicherheitskonzept **Anlage 3**). Dasselbe gilt für beabsichtigte Änderungen an in Betrieb befindlichen Anlagen. Die Einreichung ist rechtzeitig, wenn die Unterlagen spätestens drei Monate vor der beabsichtigten Einführung oder Änderung eingehen. In zwingenden Fällen kann eine kürzere Vorlaufphase in Übereinstimmung mit dem/der Behördlichen Datenschutzbeauftragten vereinbart werden.
- (2) Das Sicherheitskonzept muss den Betreiber, den Ort der elektronischen Beobachtung, den Standort des Aufzeichnungsgerätes, die Betriebszeiträume, die Art der Aufzeichnung, die Aufbewahrungsart sowie deren Ort, die Zugangsregelungen zum Aufzeichnungsgerät sowie zum aufgezeichneten Bild/Ton und die Zugangsschutzmechanismen bezeichnen.
- (3) Zugang zum Aufzeichnungsgerät dürfen nur der vom Betreiber benannte Verantwortliche und sein Stellvertreter sowie der/die Behördliche Datenschutzbeauftragte haben. Der Verantwortliche und sein Stellvertreter dürfen keine Fachvorgesetzten sein.
- (4) Die Genehmigung kann zur Sicherung der Güterabwägung sowie der Prüfung von Erforderlichkeit und Verhältnismäßigkeit ggf. mit Auflagen von dem/der Behördlichen Datenschutzbeauftragten erteilt werden.
- (5) Der Antrag ist zeitgleich über den Präsidenten an den Gesamtpersonalrat zu richten. Aufgrund des gesetzlich geforderten genehmigungspflichtigen Sicherheitskonzeptes ist ein isoliertes Mitbestimmungsverfahren nicht möglich. Sobald das bestätigte Sicherheitskonzept vorliegt, ist das Mitbestimmungsverfahren eröffnet.

§ 4 Auswertung der Aufzeichnungen, Sperrung und Löschung

- (1) Die Auswertung der Aufzeichnungen erfolgt bei erheblichen Zwischenfällen. Erhebliche Zwischenfälle sind erhebliche Störungen oder Gefährdungen von Personen, die sich im Schutzbereich der Humboldt-Universität zu Berlin befinden, oder ein erheblicher materieller Schaden für die Universität. Hierunter fallen auch Schadensersatzforderungen gegenüber der Universität.
- (2) Die Auswertung erfolgt im so genannten Vier-Augen-Prinzip durch den Behördlichen Datenschutzbeauftragten/die Behördliche Datenschutzbeauftragte und den vom Betreiber der Einrichtung benannten Verantwortlichen oder seinen Stellvertreter.
- (3) Die Auswertung ist vom Betreiber zu dokumentieren, von den Beteiligten zu unterschreiben und bei dem/der Behördlichen Datenschutzbeauftragten aufzubewahren. Zwei Jahre nach Abschluss des Verfahrens sind diese Aufzeichnungen zu vernichten.
- (4) Aufzeichnungen sind mit ihrer Entstehung zu sperren, so dass sie schon bei der Aufzeichnung nicht offen lesbar sind.
- (5) Die Aufzeichnungen sind mit Ausnahme der für die Auswertung bei Zwischenfällen erforderlichen Aufzeichnungen nach Abs. 3 spätestens sieben Tage nach ihrem Entstehen zu löschen.

§ 5 Liste der in Betrieb befindlichen elektronischen Einrichtungen für Beobachtungen

Der/die Behördliche Datenschutzbeauftragte führt eine Liste der audiovisuell-elektronischen Einrichtungen für Beobachtungen.* Dem Gesamtpersonalrat wird mindestens einmal jährlich ein vollständiges Verzeichnis dieser Einrichtungen vorgelegt, ihm werden mindestens einmal im Quartal sowie auf Anfrage sämtliche Änderungen der Einrichtungen in ausführlicher Form mitgeteilt. Die Vorlage der Unterlagen erfolgt durch den Behördlichen Datenschutzbeauftragten/die Behördliche Datenschutzbeauftragte als verzeichnisführende Stelle.

Die vollständige Liste wird gemäß § 19 BlnDSG veröffentlicht.

§ 6 Sonderregelungen für Webcams

Webcams als optisch-elektronische Geräte, die dauerhaft oder in regelmäßigen Abständen Bilder/Töne übertragen, sind nur für die Internetkommunikation zugelassen. Sie dürfen nicht zur Beobachtung mit Aufzeichnung oder am Monitor eingesetzt werden. Bereiche/Räume mit Webcams sind deutlich von außen im Eingangsbereich zu markieren (**Anlage 4**).

§ 7 Sonderregelungen für den Einsatz in der multimedialen Lehre und Forschung

Die Regelungen dieser Dienstvereinbarung gelten nicht für Teleteaching, Videokonferenzen und E-Learning, soweit die zeitlich begrenzten oder bestimmbaren Veranstaltungen als solche gekennzeichnet werden, die dadurch gewonnenen Daten nur zweckgebunden verarbeitet werden und die Daten mit einer Sperr- und Löschrfrist versehen werden. An Stelle der Sperr- und Löschrfrist kann die Archivierungsfrist treten. Mit Genehmigung des/der Behördlichen Datenschutzbeauftragten und Zustimmung der an der Aufzeichnung beteiligten Personen kann eine dauerhafte Archivierung von Videokonferenzen, Lehre im Netz o.ä. zur Dokumentation und wissenschaftlichen Auswertung zugelassen werden.

§ 8 Rechtsfolgen bei Verstößen

Bei Verstößen gegen diese Dienstvereinbarung prüfen die Dienststelle und der/die Behördliche Datenschutzbeauftragte im Rahmen ihrer Möglichkeiten dienstrechtliche, strafrechtliche und zivilrechtliche Konsequenzen. Unmittelbar nach der Feststellung eines Verstoßes werden der Gesamtpersonalrat und die zuständige örtliche Personalvertretung mit konkreter Bezeichnung der Art des Verstoßes informiert. Die in der konkreten Personaleinzelangelegenheit zuständige Personalvertretung wird über die beabsichtigten bzw. getroffenen Maßnahmen unmittelbar und zeitnah informiert.

§ 9 Übergangsregelungen

Alle Regelungen für bereits betriebene Anlagen sind auf der Grundlage der Dienstvereinbarung audiovisuell-elektronische Beobachtung zu überprüfen. Hierbei sind die sich aus der Dienstvereinbarung ergebenden Neuregelungen technisch und organisatorisch zu berücksichtigen. Innerhalb von sechs Monaten nach Unterzeichnung sind die getroffenen Regelungen in der nachgebesserten Form bei dem/der Behördlichen Datenschutzbeauftragten anzuzeigen.

§ 10 Salvatorische Klausel/In-Kraft-Treten

(1) Sollten Teile der Dienstvereinbarung für unwirksam erklärt werden, wird die Wirksamkeit der übrigen Teile nicht berührt. Die Humboldt-Universität und der Gesamtpersonalrat verpflichten sich, anstelle der unwirksamen Regelung in vertrauensvoller Zusammenarbeit eine dem gewollten Ziel möglichst nahe kommende Regelung zu treffen.

(2) Bei Bedarf ist die Dienstvereinbarung an veränderte rechtliche oder tarifvertragliche Vorschriften anzupassen. Einvernehmliche Regelungen sind jederzeit möglich.

(3) Diese Dienstvereinbarung wird für zwei Jahre abgeschlossen. Sie tritt am Tage nach der Unterzeichnung durch die Parteien oder Letztunterzeichnung in Kraft. Sofern der Verlängerung nicht spätestens drei Monate vor Ablauf der Frist von einer der Vertragsparteien widersprochen wird, verlängert sie sich jeweils um ein weiteres Jahr. Nach Kündigung wirkt diese Dienstvereinbarung bis zum Abschluss einer neuen Dienstvereinbarung gleichen Inhalts fort.

Berlin, den 30.01.2008

Berlin, den 15.02.2008

Präsident der Humboldt-Universität zu Berlin
gez. Prof. Dr. Christoph Marksches

Vorsitzender des Gesamtpersonalrats
gez. Dr. Wolfgang Mix

* Attrappen sind gegenüber dem/der Behördlichen Datenschutzbeauftragten anzuzeigen. Die Kennzeichnung erfolgt nach Anlage 1.

Anlage 1

(Organisation)



Dieser Bereich
wird
videoüberwacht!



Videoüberwachung mit Aufzeichnung

Die Aufzeichnungen werden
entsprechend der DV Video bei
Veranlassung im Beisein des
Behördlichen Datenschutzbeauftragten
der Humboldt-Universität zu Berlin
ausgewertet. Die nicht ausgewerteten
Aufzeichnungen werden regelmäßig
überspielt.

Anlage 2

Kennzeichnung für Bereiche mit Videokonferenz- oder Teleteachingausrüstung

1. Tonaufzeichnungen werden (wie gehabt) nur auf schriftlichen Auftrag der veranstaltenden Stelle gefertigt.
2. Die/der Beauftragende hat durch schriftlichen Hinweis auf dem Podium auf die Tonaufzeichnung aufmerksam zu machen.
3. Schilder werden von dem Referat für Öffentlichkeitsarbeit und von der Technischen Abteilung bereitgehalten und sind über das Internet als Papierform abrufbar.
4. Ist aus der Aufnahme die Aufklärung über die Tatsache der Tonaufnahme nicht ersichtlich, bzw. ist durch einen anderen Hinweis der Verdacht gegeben, dass die alternativ mögliche visuelle Aufklärung unterblieben ist, so darf die Tonaufzeichnung nicht herausgegeben werden.
5. Die Herausgabe der Aufzeichnung erfolgt gegen Quittung.
6. Die Quittung beinhaltet auch die Erklärung des/der Beauftragenden, dass die visuelle Aufklärung vorgenommen wurde.

Muster für Quittung

Ich habe heute von der Technischen Abteilung

... Tonbandkassetten

mit Mitschnitten der Veranstaltung vom

erhalten.

Die Teilnehmer der Veranstaltung waren von dem Veranstalter über den Tonmitschnitt unterrichtet.

Datum, Unterschrift, Name und Einrichtung in Blockschrift

A) Muster für auditive Aufklärung

Die Veranstaltung

wird für eigene

Zwecke tontechnisch

aufgezeichnet.

B) Muster für Videoaufzeichnung

**Die Veranstaltung
wird für eigene
Zwecke
videotechnisch
aufgezeichnet.**

C) Videokonferenz

**Videokonferenz zu
wissenschaftlichen
Zwecken
mit/ohne
Aufzeichnung**

D) Teleteaching

1.

**Teleteaching-
Veranstaltung
mit/ohne**

Videoaufzeichnung

2.

In diesem Raum findet eine
Teleteaching-Veranstaltung
über das Internet statt. Beim
Betreten des Raumes
können Sie in den Focus
einer Kamera gelangen und
Ihr Bild könnte weltweit
übertragen werden.

Anlage 3

Aufbau des Sicherheitskonzeptes und der Darlegung der Erforderlichkeit und der Verhältnismäßigkeit

Betreiber

Ort der elektronischen Beobachtung

Standort des Aufzeichnungsgerätes

Betriebszeiträume

Art der Aufzeichnung

Darlegung der technisch-organisatorischen Maßnahmen zum Datenschutz

1. Vertraulichkeit

Nur Befugte haben Zugang zu dem per Video oder Tontechnik erlangten Datenmaterial. Die Verantwortlichen sind im Voraus festzulegen. Die Festlegung ist zu dokumentieren und bei dem/der Behördlichen Datenschutzbeauftragten zu hinterlegen. Bei der Auswertung gelten grundsätzlich das Vier-Augen-Prinzip und die Dokumentationspflicht über die Auswertung (Zugangsregelungen zum Aufzeichnungsgerät sowie zum aufgezeichneten Bild/Ton und die Zugangsschutzmechanismen, Benennung der Verantwortlichen).

2. Integrität

Die Daten müssen während der Verarbeitung unversehrt, vollständig und aktuell bleiben.

3. Verfügbarkeit

Geeignete Maßnahmen zum Schutz der Daten gegen Verlust oder Zerstörung, z. B. Datensicherung und Notfallvorsorge, Protokollierung, Arbeitsablaufsbeschreibungen, Dienstanweisungen (Aufbewahrungsart der Daten sowie deren Ort).

4. Authentifizierung

Die Daten müssen jederzeit ihrem Ursprung zugeordnet werden können.

5. Revisionsfähigkeit

(Automatisierte) Eingabekontrolle durch Protokollierung. Nur so können die Umstände aufgeklärt werden, die (versehentlichen) Fehleingaben oder Manipulationen zu Grunde liegen. Aber auch die rechtmäßige Nutzung ist zu dokumentieren (s.a. 1.; Mitbestimmung des Gesamtpersonalrats!)

6. Transparenz

Protokollierung der für Datenschutz und Datensicherheit relevanten Abläufe. Ebenfalls zur datenschutzgerechten Organisation gehören Regelungen zum Umgang mit den technischen Sicherheitseinrichtungen, zur Akten- und Datenträgervernichtung, zur Löschung und Sperrung von Daten, zur Gewährleistung der Betroffenenrechte (z. B. Auskünfte, Benachrichtigungen).

Informationsrecht des/der Behördlichen Datenschutzbeauftragten, Informationsrecht des Landesdatenschutzbeauftragten, Auskunftspflicht gegenüber Interessierten ("Jedermann").

7. Prüfung der Erforderlichkeit und Verhältnismäßigkeit

Der Einsatz von Videoanlagen muss geeignet, notwendig und verhältnismäßig im engeren Sinne sein. Geeignet ist die Maßnahme, wenn sie den erstrebten Erfolg überhaupt zu erreichen vermag; geeignet ist das Mittel, wenn es kein anderes, den Betroffenen und die Allgemeinheit weniger beeinträchtigendes Mittel gibt. Außerdem darf das Mittel nicht außer Verhältnis zum erstrebten Erfolg sein.

Anlage 4



In diesem Raum werden
Webcams eingesetzt.
Eine Überwachung oder
Aufzeichnungen mittels
Webcam finden nicht
statt.