dsb
datenschutzbeauftragter
kanton zürich

www.datenschutz.ch

# Allgemeine Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen

(AGB Auslagerung Informatikleistungen)

## 1. Anwendungsbereich

Diese AGB sind Bestandteil des Vertragsverhältnisses zwischen dem öffentlichen Organ (Auftraggeber) und dem Auftragnehmer, welches die Auslagerung der Bearbeitung von Personen- und Sachdaten (Informationen) im Rahmen von § 6 Gesetz über die Information und den Datenschutz (IDG, LS 170.4) i.V.m. § 25 Verordnung über die Information und den Datenschutz (IDV, LS 170.41) unter Inanspruchnahme von Informatikleistungen zum Gegenstand hat. Als öffentliche Organe gelten die Behörden und Organisationen i.S.v. § 3 Abs. 1 IDG.

## 2. Verantwortung

Das öffentliche Organ ist für die Bearbeitung der Informationen verantwortlich. Der Auftragnehmer ist lediglich im Rahmen der vertraglichen Vereinbarung ermächtigt, die Informationen des öffentlichen Organs zu bearbeiten.

## 3. Rechtliche Verfügungsmacht über die Informationen

Das öffentliche Organ behält die vollumfängliche Verfügungsmacht über die bearbeiteten Informationen. Es kann dem Auftragnehmer insbesondere ohne Begründung und ungeachtet der konkreten vertraglichen Situation jederzeit den Zugriff auf die bearbeiteten Informationen untersagen, diese unentgeltlich in einem zum voraus vereinbarten Format herausverlangen oder den Auftragnehmer auffordern, die bearbeiteten Informationen bei sich unwiderruflich zu löschen.

## 4. Zweckbindung

Die vom Auftragnehmer bearbeiteten Informationen dürfen ausschliesslich zum vertraglich festgelegten Zweck verwendet werden. Weitere Verwendungszwecke müssen vom öffentlichen Organ schriftlich bewilligt werden.

## 5. Bekanntgabe von Informationen

Die Bekanntgabe von Informationen an Dritte erfolgt ausschliesslich im Rahmen der vertraglichen Vereinbarung oder nach schriftlicher Ermächtigung des öffentlichen Organs.

Sollte der Auftragnehmer aufgrund einer richterlichen Zwangsmassnahme verpflichtet werden, den zuständigen Behörden Zugang zu Systemen und Informationen des öffentlichen Organs zu verschaffen, informiert er dieses unverzüglich.

## 6. Geheimhaltungspflichten

Der Auftragnehmer, dessen Mitarbeitende und Unterauftragnehmer unterstehen im Rahmen der Vertragserfüllung der umfassenden Geheimhaltungs- und Schweigepflicht des Amtsgeheimnisses. Vorbehalten bleiben weitergehende gesetzlich verankerte Schweigepflichten (beispielsweise Berufsgeheimnisse).

Diese Geheimhaltungspflichten beziehen sich auf alle Systeme, Prozesse und Informationen des öffentlichen Organs und gelten auch innerhalb des Unternehmens des Auftragnehmers, ungeachtet der hierarchischen Positionen.

Wenn die Auslagerung das Bearbeiten von besonderen Personendaten beinhaltet, werden diese von Mitarbeitenden des Auftragnehmers oder des Unterauftragnehmers bearbeitet, die diesbezüglich dem Kontroll- und Weisungsrecht des öffentlichen Organs unterstellt sind, es sei denn, organisatorische und technische Massnahmen verhindern eine Kenntnisnahme.

## 7. Informationszugangsgesuche

Der Auftragnehmer leitet Informationszugangsgesuche i.S.v. § 20 IDG umgehend an das öffentliche Organ weiter, ohne diese selbst zu beantworten. Der Auftragnehmer trifft Vorkehrungen, um dem öffentlichen Organ die Beantwortung der Anfragen zu ermöglichen.

Die Durchsetzung der Rechte Betroffener auf Berichtigung und Löschung ist durch den Auftragnehmer garantiert.

## 8. Informationssicherheit

### a. Allgemeines

Der Auftragnehmer kennt die Pflicht des öffentlichen Organs, Informationen durch angemessene organisatorische und technische Massnahmen zu schützen (§ 7 IDG). Das öffentliche Organ orientiert den Auftragnehmer über den Schutzbedarf der zu bearbeitenden Informationen.

Zur Sicherstellung der Informationssicherheit unterhält der Auftragnehmer ein Sicherheitsmanagement, abgestuft nach dem Schutzbedarf der Informationen. Er erstellt eine Sicherheitsorganisation und ein Sicherheitskonzept, damit die Informationssicherheit im laufenden Betrieb aufrecht erhalten und ständig verbessert wird. Es

gelten die Standards der ISO/IEC 27000-Serie oder des BSI Grundschutzstandards 100-1 bis 100-4.

### b. Trennung der Informationsbestände

Der Auftragnehmer trifft die notwendigen organisatorischen und technischen Massnahmen, um die Informationen des öffentlichen Organs von denjenigen anderer Auftraggeber zu trennen.

### c. Informationspflicht des Auftragnehmers

Der Auftragnehmer informiert und dokumentiert das öffentliche Organ über die Methoden und Prozesse, die er zur Einhaltung der Informationssicherheit einsetzt. Das öffentliche Organ hat das Recht, weiterführende Unterlagen einzusehen und sich die betrieblichen Abläufe vorführen zu lassen.

Weiter ist das öffentliche Organ über besondere Vorkommnisse (Datenverlust, Hackerangriff, unrechtmässige Zugriffe) umgehend zu informieren. Es sind formale Meldeverfahren mit Ansprechpersonen festzulegen.

## 9. Kontrolle

### a. Sicherheits-Audits

Der Auftragnehmer ist verpflichtet, periodische Sicherheits-Audits nach anerkannten Audit-Standards (beispielsweise: Schweizerische Kammer der Wirtschaftsprüfer und Steuerexperten, Information Systems Audit and Control Association, ISACA) durch unabhängige Prüfstellen durchzuführen. Auf Anfrage stellt er dem öffentlichen Organ die Berichte unentgeltlich zur Verfügung.

### b. Kontrolle durch unabhängige Aufsichtsbehörden

Der Auftragnehmer untersteht der Aufsicht der Kontrollorgane des öffentlichen Organs, namentlich der oder dem Datenschutzbeauftragten oder der Finanzkontrolle. Der Auftragnehmer hat den Kontrollorganen des öffentlichen Organs Zugang zu dessen Informationen, Systemen und Prozessen zu verschaffen, diese unentgeltlich zu unterstützen sowie die notwendigen zeitlichen und fachlichen Ressourcen zur Verfügung zu stellen.

## 10. Unterauftragsverhältnisse

Der Auftragnehmer darf Dritte zur Erfüllung seines Auftrages nur beiziehen, wenn das öffentliche Organ schriftlich zugestimmt hat oder er diese zu Beginn des Auftragsverhältnisses offen gelegt hat. Der Unterauftragnehmer muss sämtliche Pflichten aus dem Vertragsverhältnis sowie aus diesen AGB rechtsgültig übernehmen.

## 11. Entwicklung und Wartung von Systemen

Erfordert die Entwicklung und Wartung von Systemen den Beizug Dritter, verhindert der Auftragnehmer durch organisatorische und technische Massnahmen, dass den Dritten Informationen des Auftraggebers zur Kenntnis gelangen. Lässt sich dies or-

ganisatorisch und technisch nicht verhindern, gelten die Bestimmungen über Unterauftragsverhältnisse.

**12. Ort der Datenbearbeitung / gleichwertiges Datenschutzniveau**

Die Verarbeitungsprozesse mit Informationen des öffentlichen Organs sowie deren Speicherung und Archivierung haben grundsätzlich in der Schweiz zu erfolgen.

Das Bearbeiten von Personendaten ausserhalb der Schweiz darf ausschliesslich in einem Land mit angemessenem Datenschutzniveau erfolgen (analog § 19 IDG i.V.m. § 22 IDV). Das öffentliche Organ hat dies schriftlich zu bewilligen. Inhalt und Ort der Informationsbestände sind aktuell zu dokumentieren.

**13. Cloud Computing**

Bei der Nutzung von Cloud Services sind zusätzlich folgende Anforderungen zwingend zu beachten:

- Der Auftragnehmer informiert und dokumentiert den Auftraggeber schriftlich und umfassend über die eingesetzte Technologie bzw. über eine Weiterentwicklung der eingesetzten Technologie.

- Der Auftragnehmer informiert das öffentliche Organ über sämtliche mögliche Datenbearbeitungsorte.

- Sämtliche Informationsbestände mit besonderen Personendaten dürfen nur mit einer umfassenden kryptographischen Sicherung in die Cloud einfliessen. Der Auftragnehmer stellt die erforderlichen kryptografischen Massnahmen während dem gesamten Bearbeitungsprozess – bis und mit Löschung oder Vernichtung – sicher. Das öffentliche Organ verwaltet die notwendigen Zertifikate (Schlüssel) selbst.

- Die Massnahmen zur Gewährleistung der Portabilität, Interoperabilität richten sich nach der vertraglichen Vereinbarung.

**14. Wahrung von Geschäftsgeheimnissen des Auftragnehmers**

Das öffentliche Organ verpflichtet sich, die Geschäftsgeheimnisse des Auftragnehmers zu wahren.

**15. Werbung**

Werbung und Veröffentlichungen über vertragsspezifische Leistungen bedürfen der schriftlichen Zustimmung des öffentlichen Organs.

**16. Sanktionen**

Bei schwerwiegender Verletzung einer Bestimmung des Vertrages oder dieser AGB Auslagerung Informatikleistung zahlt die verletzende Partei der verletzten Partei eine Konventionalstrafe, sofern sie nicht beweist, dass sie kein Verschulden trifft. Die Höhe richtet sich nach der vertraglichen Vereinbarung. Vorbehalten bleibt der Ersatz

des darüber hinaus gehenden Schadens. Bei wiederholter schwerwiegender Verletzung steht der verletzten Partei das Recht zur sofortigen Vertragsauflösung zu. Der daraus entstehende Schaden ist ihr zu vergüten.

Die Bezahlung der Konventionalstrafe befreit nicht von den Geheimhaltungspflichten.

Vorbehalten bleiben strafrechtliche Sanktionen.

**17. Vertragsauflösung**

Ungeachtet des Grundes der Vertragsauflösung verpflichtet sich der Auftragnehmer, die für das öffentliche Organ bearbeiteten Informationsbestände unentgeltlich im vereinbarten Format umgehend zu übertragen. Die Pflichterfüllung kann vom Auftragnehmer selbst dann nicht aufgeschoben werden, wenn zwischen den Parteien Auseinandersetzungen bestehen sollten.

Das öffentliche Organ kann vom Auftragnehmer die unentgeltliche Vernichtung der im Rahmen des Auftragsverhältnisses bearbeiteten Informationsbestände verlangen. Die diesbezügliche Pflichterfüllung kann es selbst überprüfen oder durch einen Dritten überprüfen lassen.

Auch nach der Vertragsauflösung ist der Auftragnehmer, dessen Mitarbeitende bzw. allfällige Unterauftragnehmer an die Geheimhaltungspflicht gebunden.

**18. Anwendbares Recht**

Es gilt das im Vertrag vereinbarte schweizerische Recht.

**19. Gerichtsstand**

Es gilt der Gerichtsstand des öffentlichen Organs.

August 2012