Verfahrensverzeichnis
(§ 4g Abs. 2 BDSG)

I. Angaben zur verantwortlichen Stelle (§ 4e Satz 1 Nr. 1-3 BDSG)

Nr. 1 Name oder Firma der verantwortlichen Stelle:
dna Gesellschaft für IT Services mbH / HRecruiting
Nr. 2 Leiter der verantwortlichen Stelle und der Datenverarbeitung:
Geschäftsführer: Oliver Schuppart
Nr. 3 Anschrift der verantwortlichen Stelle:
Am Kaiserkai 10 20457 Hamburg
Kontaktdaten des Datenschutzbeauftragten (falls nach § 4 f BDSG zu bestellen):
Volker Hempen Mail: volker.hempen@dna-gmbh.de Tel 040-41263141 Fax 040-41263140

II. Angaben zu den Verfahren automatisierter Verarbeitung (§ 4e Satz 1 Nr. 4-8 BDSG)

Nr. 4 Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung:
• Bewerberverwaltung • Begründung der Rechtmäßigkeit der Verarbeitung aus Vertragsverhältnis • Phasen der Datenverarbeitung: Erhebung, Speicherung und Nutzung • Herkunft der Daten: Übermittlung • Backup-Regelung: Datenträger • Art der eingesetzten Datenverarbeitungsanlage: Client/Server, öffentl. Netz, verschlüsselte Datenübertragung im Internet

- Kurzcharakteristik der Datenverarbeitungsanlage:

  Das HRecruiting System wird webbasiert als ASP-Lösung (Application Service Provider) realisiert. Es werden neben der Bewerberinformation, Bewerberdatenaufnahme und Tauglichkeitstests auch die prozessunterstützenden und administrative Funktionalitäten für die Sachbearbeitung der Personalfachabteilungen webbasiert zur Verfügung gestellt. Alle Daten werden dazu in einem relationalem Datenbanksystem gespeichert. Dabei sind aus Sicherheits- und Performancegründen mehrere Datenbanken geclustert (d.h. mehrere sich replizierende Datenbanken). Diese laufen parallel auf mehreren Servern (Produktiv- und Backup - System) im abgesicherten Rechenzentrum von MCS, Hamburg. Zusätzlich steht ein Notfall/Ersatzsystem in einer aktuellen Konfiguration (ohne Daten) als dediziertes System in einem Rechenzentrum bei der Hetzner Online AG, Gunzenhausen. Die Datensicherung erfolgt redundant durch online Replizierung, Online Backup in SQL Dumps sowie deren zusätzliche Sicherung auf ein Offlinedatenträgersystem bei MCS. Die einzelnen Sicherungsstandorte befinden sich in unterschiedlichen Brandschutzabschnitten. Die Produktivsysteme werden nach außen von einem dedizierten Check Point NGX HA-Cluster aktueller Version geschützt, das alle Zugriffe auf produktionsirrelevante Ports abwehrt. Logfiles werden täglich gewechselt und gesichert (Logrotate) und automatisiert nach Auffälligkeiten geprüft. Zusätzlich ist die Webanwendung durch ein Intrusion Detection geschützt. Werden verdächtige Eingaben registriert, wird die Verarbeitung abgebrochen und eine Mail an die Administratoren versandt. Der Aufbau des Systems ist in einer „Drei Schichten Architektur“ realisiert:

1st Layer - Darstellungsschicht: HTML + Javaskript im Browser
2nd Layer - Businesslogik-Schicht: PHP
3rd Layer - Datenbank Schicht: mySQL Datenbank als Cluster

  Die Systemsicherheit wird durch eine Update/Patch Datenbank des Betriebssystem Herstellers sowie in einem wöchentlichen Audit in einschlägigen Foren Hinweisen auf Security Patches nachgegangen.
  Der Zugriff auf das System erfolgt ausschließlich über HTTPS (Port 443). Reiner Content (Stellenbeschreibungen) wird unverschlüsselt per HTTP (Port 80) übertragen.
  Der Zugriff auf personenbezogene und unternehmensinterne Daten erfolgt über eine verschlüsselte Datenverbindung (128 Bit SSL).
  Die Authentifizierung am Anwendungssystem erfolgt datenbankbasiert.

Nr. 5 Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten- oder Datenkategorien:

Personengruppe	Daten/Datenkategorie
Bewerber	Name, Adressdaten, beruflicher Werdegang vertraulich

Nr. 6 Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können:

dna GmbH
Auftragsdatenverarbeitung nach § 11 BDSG

Nr. 7 Regelfristen für die Löschung der Daten:
Löschung der Bewerberdaten nach 6 Monaten
Nr. 8 Geplante Datenübermittlung in Drittstaaten:
geplant: nein