

Datenschutz im Hogrefe TestSystem

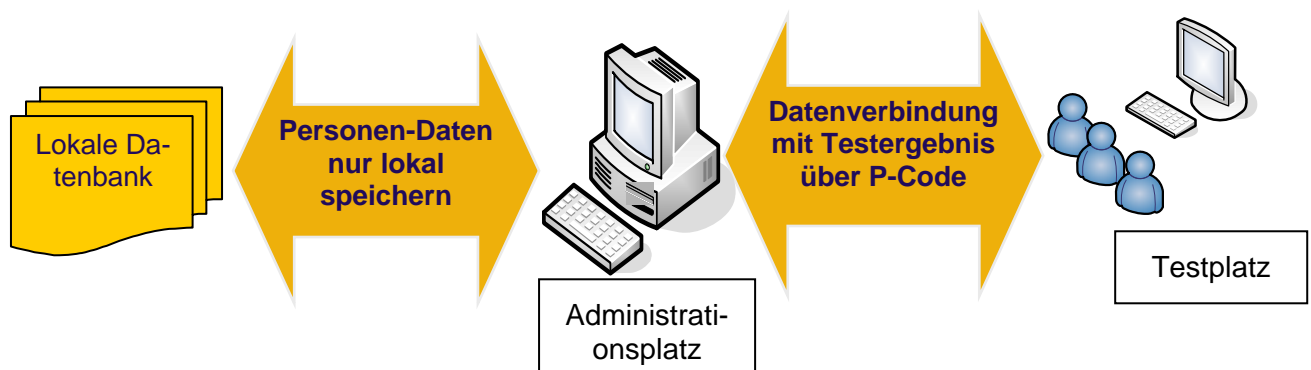
Das Prinzip „*Der beste Datenschutz ist die Vermeidung schutzwürdiger Daten*“ kann mit dem **Hogrefe TestSystem (HTS)** umgesetzt werden. Es ist grundsätzlich **nicht notwendig**, schutzrelevante Daten im HTS zu erfassen. Lediglich **Alter in Jahren und Geschlecht** sind für die Anwendung der zutreffenden Normen bei einigen Tests notwendig – die aber für sich genommen keine Identifikation einer Person ermöglichen. Die Identifikation der Person für den Diagnostiker kann über einen individuellen Code (I-Code, z.B. die Nummer in einer eigenen Probandenverwaltung) eingegeben werden – bzw. es kann der automatisch in HTS vergebene einmalige Personen-Code (P-Code) verwendet werden. Die Dokumentation der Zuordnung Ergebnis zur Person kann ausserhalb des HTS erfolgen.

Verwendet man einen fest installierten HTS-Administrationsplatz, werden **lokale Datenbanken** verwendet, wo datenschutzrelevante Informationen der Personen eingegeben werden können, um die Personen genauer zu dokumentieren (Name, Geburtsdatum, Adresse, Sozialdaten usw.). Diese Datenbanken können auf dem lokalen PC zugänglichen Datenträgern gespeichert werden und es sind die üblichen Schutzmassnahmen (Zugangssicherung zum PC und zu den Datenträgern) zu ergreifen. Die Datenbanken selbst sind allerdings verschlüsselt (mit Kennwortschutz) und nur durch ein Hogrefe TestSystem interpretierbar. Eine solche Datenbank kann nicht gelesen werden, wenn Sie in unberechtigte Hände gelangt.

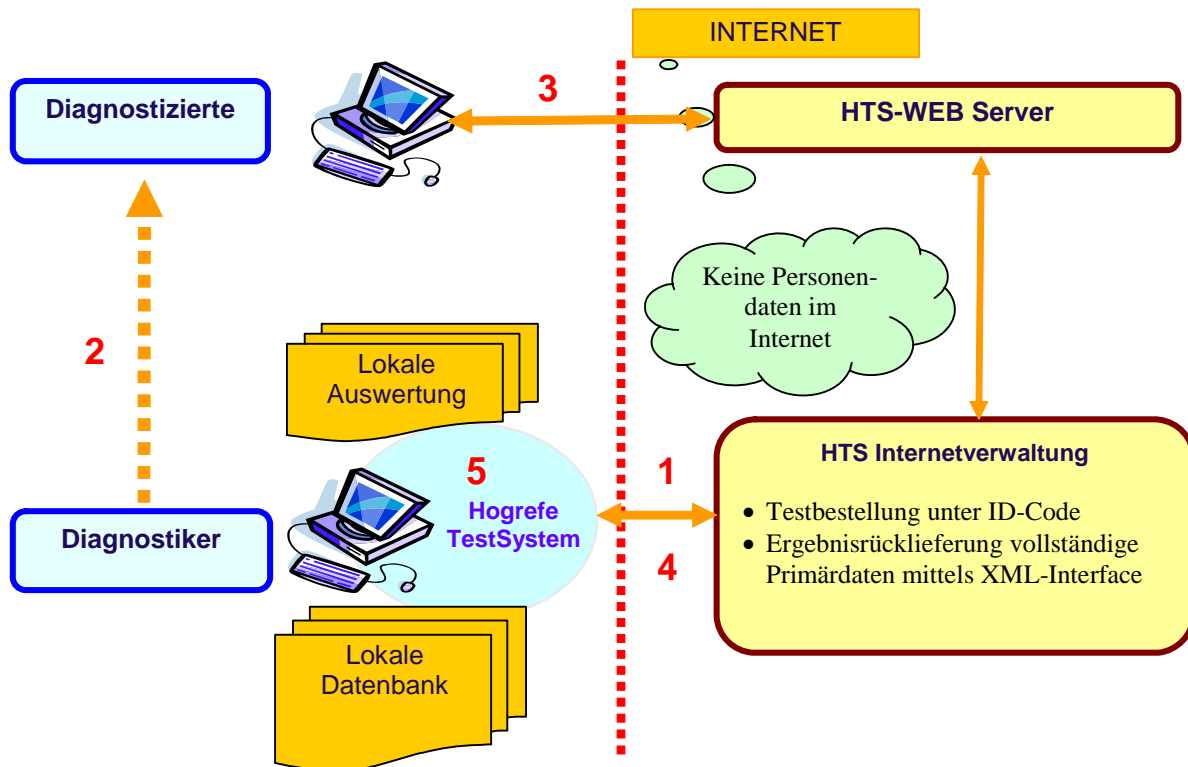
Das HTS ist mandantenfähig und die Anmeldung der HTS-Benutzer kann kennwortgeschützt erfolgen. Es besteht auch die Möglichkeit, „persönliche Datenbanken“ anzulegen. Diese kann dann nur der jeweilige Benutzer lesen, ein Lesen mit einem anderen Hogrefe TestSystem – oder auch am gleichen System durch einen anderen Benutzer - ist nicht möglich.

Bei **Internet Testing, Intranet Testing bzw. Portable Testing** besteht die Möglichkeit, an einem anderen PC als dem lokalen HTS-Administrationsplatz die Tests durchzuführen. Die Kommunikation Administrationsplatz – Testplatz erfolgt über einen **Server** (Internet, Intranet bzw. mobiler Server auf einem USB-Memorystick).

Es ist mit dem sogenannten **individuellen Testen** (Person wird vorher im lokalen HTS erfasst) mit allen genannten Testarten realisierbar, dass keine persönlichen Daten den lokalen PC mit dem HTS-Administrationsplatz verlassen und sich auf dem Server wiederfinden. Die Verbindung der Testung mit der Person erfolgt über den einmaligen und vom System vergebenen P-Code. Erst die fertige Messung wird in der lokalen Datenbank wieder mit den Personendaten verbunden.



Für das individuelles Testen im Internet stellt sich der Ablauf folgendermassen dar:



1. Bestellung von Internettests für Personen: Ins Internet werden nur (einmalig vergebene) ID-Codes (P-Code liegt dem zugrunde) zur Identifikation übergeben, alle sonstigen Personendaten bleiben lokal. Da die Lizenzierung der Tests ebenfalls lokal erfolgt, müssen auch keine personalisierten Abrechnungsdaten übermittelt werden;
2. Übermittlung der Zugangsdaten zur Diagnostik im Internet an die Diagnostizierten, welche im Schritt 1 zurückgemeldet wurden;
3. Anmeldung am HTS-WEB-Server www.htsonline.net mit den Zugangsdaten durch die Diagnostizierten und Durchführung der Tests;
4. Die vollständigen Primärdaten der Tests (also Itemantworten, Einzel-Zeiten) werden ins HTS zurückgeladen (XML-Interface) und anhand des ID-Codes wieder mit der Person verbunden. Für Internettests stehen also gleich ausführliche Informationen zur Verfügung wie für lokal durchgeführte Tests;
5. Die Testergebnisse können ggf. mehrfach nach verschiedensten Gesichtspunkten lokal ausgewertet werden (dadurch auch maximale Auswerteflexibilität) und die Befunde im Diagnoseprozess verwendet werden.

Die Vorteile der Verwendung einer lokalen Datenbank für Ergebnisse beim Diagnostiker sind noch einmal zusammengefasst:

- Keine schutzrelevanten Personendaten gelangen ins Internet bzw. müssen auf der Seite des Internet-Testanbieters verwendet werden;
- Die Möglichkeit mehrfacher Auswertungen (auch mit verschiedenen Normen, in verschiedener Ausführlichkeit) besteht, auch spätere Auswertungen oder vergleichende Darstellungen mehrerer Personen sind jederzeit möglich;

- Die Aufbewahrungsmöglichkeit der Daten für entsprechende Nachweis- und Dokumentationszwecke – die bei Rückfragen und Rekursen u.U. Einsicht in das genaue Antwortprotokoll notwendig machen, ist möglich;
- Die (ggf. hier anonymisierte) Aufbewahrungsmöglichkeit der Primärdaten für eigene Forschungs- und Normierungszwecke ist gewährleistet.

Der **Intranet-Server** funktioniert ebenso. Auch beim **Portable Testing** verlassen keine Personendaten den PC, wenn klassisches individuelles Testen gewählt wird.

Die Verbindungen zwischen Web- Administrationsplatz und Server auf der einen sowie Testplatz und Server auf der anderen Seite erfolgen über gesicherte SSL-Verbindungen. Beim Portable Testing ist der USB-Stick entsprechend zu schützen.

Es ist allerdings beim individuellen wie beim seriellen Testen (letzteres ohne vorheriges Anlegen der Person) **auch möglich, Personendaten von der Person direkt zu erfragen oder im lokalen HTS bereits gespeicherte Daten der Person zur Überarbeitung zu übersenden**. Hier verlassen diese Daten den lokalen PC –dies ist allerdings ein Erfordernis der Praxis.

Für die generelle Verwendung von Personendaten im diagnostischen Prozess (Eingabe von Namen, Geburtsdaten, Adressdaten u.ä. während der Testung) trägt daher der Diagnostiker die Verantwortung und muss das Einverständnis für die Erhebung und Speicherung ggf. einholen bzw. den für ihn geltenden rechtlichen Rahmen berücksichtigen.

Die "International Guidelines on Computer-Based and Internet Delivered Testing"¹ der **Internationalen Testkommission** (ITC), fordern lediglich " einen sicheren Transfer für Getestete (z.B. SSL) und die Aufrechterhaltung der Vertraulichkeit der Resultate".

Die **Internet-Server** stehen bei qualifizierten Providern, die Zugangsrechte für Wartung und Weiterentwicklung sind entsprechend der üblichen Datenschutzrichtlinien geregelt (Zutrittskontrolle, Zugangskontrolle). Die Datensicherheit wird durch entsprechende Backup-Verfahren und redundante Systeme gewährleistet.

Bitte beachten Sie, dass auch der **Testschutz** mit zum Datenschutz gehört. Wenn Tests für Fragestellungen eingesetzt werden, von denen eine Entscheidung abhängt, sollten die Items der Tests nicht öffentlich bekannt werden – sonst sind Ergebnisse ggf. nicht verwendbar. Professionelle Testverfahren unterliegen kontrollierten Vertriebsbedingungen, die einen gewissen Schutz bieten. Dies gilt auch für IT-basierte Testverfahren. Wo immer möglich, sollten Sie wichtige Testdurchführungen unter kontrollierten Bedingungen durchführen. Dazu gehört

- ggf. Identitätsprüfung der Person (bei prüfungsartigen Anlässen, wenn die Person nicht persönlich bekannt ist)
- Beaufsichtigung der Testdurchführung (an entfernten Orten ggf. durch eine beauftragte Vertrauensperson und Verhinderung unerlaubter Hilfsmittel und Kommunikation).

Prof. Dr. Klaus-Dieter Hänsgen, Direktor des ZTD
 ZTD Zentrum für Testentwicklung und Diagnostik am
 Departement für Psychologie der Universität Fribourg
 UNI Rte Englisberg 9, CH-1763 GRANGES-PACCOT
 E-Mail: Klaus-dieter.haensgen@unifr.ch

¹ Siehe <http://www.intestcom.org/>