

---

*The Background Screening Credentialing Council (BSCC) has drafted the following accreditation tip for the US Employment Screening / General Background Screening BSOAP Standard, this tip applies to US Version 2.0, 3.0 and General Version 1.0. This response is provided for educational purposes only and does not constitute legal advice, express or implied of the BSCC, or the Professional Background Screening Association. Consultation with legal counsel is recommended in all matters of employment law.*

*For the purposes of this Tip, and to ensure our response applies to both Standards, the terms Organization and CRA may both be used.*

---

**TITLE: Clause 3.4 Information Protection**

*US Clause: CRA must have and follow a procedure to inform client of: (1) the sensitive nature of consumer reports, (2) the need to protect such information, and (3) the consumer report retention and destruction practices as outlined in the federal FCRA and the DPPA.*

*General Clause: Organization must have and follow a procedure to inform client of: 1) the sensitive nature of subject reports, 2) the requirement to protect such information, and 3) the subject report retention and destruction practices as outlined in the Fair Information Privacy Principles (FIPPs).*

A **Non-Conformity** for Clause 3.4 may look something like the following:

The absence of specific language in a client agreement or other document *signed by the client* that includes information regarding the importance of and legal requirements to protect consumer data presented in consumer reports as per the FCRA and DPPA. Clause 1.11 of the Standard outlines requirements for proper data destruction. Documentation must require all consumer and client information to be destroyed and disposed of securely as to render information inaccessible, unreadable, and unrecoverable. Further, the requirement must go beyond just notification to the client of these responsibilities but requires their signed acknowledgement of these requirements.

The Audit Criteria for 3.4 provides:

*[US Standard] CRA must inform clients of client's legal requirements regarding protection of consumer data. Methods include, but are not limited to, inclusion in a Client agreement, User agreement or through some other document which is signed by the client and includes, but is not limited to, client acknowledgement of consumer data protection responsibilities. Per the FCRA, current requirements include: 1) limiting dissemination of consumer information to only those with legitimate need, permissible purpose, and authorized by consumer; 2) retaining consumer data in a confidential manner; and 3) destroying data in a secure manner as specified in current FTC document destruction rules. Per the DPPA, current requirements include protecting the privacy of consumer information which is contained in*

*motor vehicle records, and accessing DMV records only with written consent of consumer. Auditor will seek evidence of adherence to policies and procedures.*

[Global Standard] Organization must inform clients of client's legal requirements regarding protection of subject data. Methods include, but are not limited to, inclusion in client agreement, user agreement or through some other document which is signed by the client and includes, but is not limited to, client acknowledgement of subject data protection responsibilities. Per the FIPPs, current requirements include: 1) limiting dissemination of subject information to only those with legitimate need, permissible purpose, and authorized by subject, 2) retaining subject data in a confidential manner, and 3) destroying data in a secure manner.

We hope the above provides further information and clarification on the information provided in the Standard and may be used to improve your accreditation submission.